УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

Перица Б. Милетић

ОРГАНИЗАЦИОНО И НОРМАТИВНО УРЕЂЕЊЕ ЗАШТИТЕ ИНФОРМАЦИЈА У ФУНКЦИЈИ БЕЗБЕДНОСТИ ПОСЛОВАЊА БАНАКА И ФИНАНСИЈСКИХ ИНСТИТУЦИЈА

ДОКТОРСКА ДИСЕРТАЦИЈА

Београд, 2020.

UNIVERSITY OF BELGRADE

FACULTY OF SECURITY STUDIES

Perica B. Miletić

ORGANISATIONAL AND PRESCRIPTIVE REGULATION OF INFORMATION PROTECTION FOR OPERATIONS SECURITY OF BANKS AND FINANCIAL INSTITUTIONS

Doctoral Dissertation

Belgrade, 2020.

Ментор:

Др Горан Ј. Мандић, ванредни професор, Универзитет у Београду, Факултет безбедности

Чланови комисије:

Др Бранкица Поповић, ванредни професор, Криминалистичко-полицијски универзитет

Др Ненад Путник, ванредни професор, Универзитет у Београду, Факултет безбедности

Др Миленко Ћелетовић, ванредни професор, Универзитет у Београду, Факултет безбедности

Датум одбране: _____

ОРГАНИЗАЦИОНО И НОРМАТИВНО УРЕЂЕЊЕ ЗАШТИТЕ ИНФОРМАЦИЈА У ФУНКЦИЈИ БЕЗБЕДНОСТИ ПОСЛОВАЊА БАНАКА И ФИНАНСИЈСКИХ ИНСТИТУЦИЈА

Глобална повезаност националних и регионалних економских система један је од неупитних карактеристика савременог друшва, где пословање банака и финансијских институција има кључну улогу у остваривању овог система. Пословање ових субјеката у великој мери је зависно од очувања потребних ресурса за редовно пословање, а информације у том смислу представљају можда и најважнију вредност и предмет заштите.

Нова технолошка револуција коју доноси процес дигитализације свих сегмената друштва, дакле и сферу пословања, потенцира значај који имају информације као стратешки ресурс за пословање банака и финансијских институција. Без обраде података и информација неби било могуће обављати пословне процесе, а савремено пословање захтева обраду све веће количине информација и њихову бржи обраду и већу доступност корисницима, што може довести до веће рањивости информација и угрожавања пословања.

Заштита информација у банкама и финансијским институцијама, посматрано са аспекта организационог и нормативног уређења ове области, има за циљ да допринесе превазилажењу недоследности које се јављају у практичном остваривању пословне функције заштите информација, у смислу фаворизовања техничког аспекта сагледавања проблема заштите информација на рачун других – нетехничких аспеката. Ова недоследност је предмет научних радова који се јављају у последњих двадесетак година, о чему су у раду изнети одговарајући докази. Такође, теорија је сагласна да се заштита информација бави заштитом информатичких ресурса, људи и пословних процеса, што представља још један аргумент о потреби сагледавања комплетне слике заштите информација, не губећи при томе из вида значај који имају информатички ресурси и технички аспект проблема, али и истовремено отвара питања на који начин је могуће допринети заштити информација у погледу других аспеката. Из тих разлога, у раду је посматрано организационо и нормативно уређење заштите информација у банкама и финансијским институцијама, као допринос изградњи функционалнијих система безбедности ових привредних субјеката.

У раду је извршена анализа до сада објављених научних сазнања која се односе на област заштите информација у банкама и финансијским институцијама, посматрано са организационог и нормативног аспекта, којом приликом је у одговарајућим поглављима сагледан теоријски концепт заштите информација и дат преглед нормативног оквира предметне области на националном и међународном нивоу. Такође, у раду је наглашена потреба развоја безбедности свести свих запослених о потреби заштите информација, будући да људи, са својим ставовима, знањима и понашањем, представљају најбољи механихизам заштите и највећи извор угрожавања, одакле области организационе културе, посебно безбедносне културе

добијају на свом значају за развој система заштите информација у банкама и финансијским институцијама.

Кључне речи: заштита информација, безбедност, заштита информација у банкама и финансијским институцијама, организационо уређење заштите информација, нормативно уређење заштите информација, организација, безбедносна култура

Научна област: интердисциплинарне, мултидисциплинарне и трансдисциплинарне студије

Ужа научна област: студије безбедности

УДК број:

ORGANISATIONAL AND PRESCRIPTIVE REGULATION OF INFORMATION PROTECTION FOR OPERATIONS SECURITY OF BANKS AND FINANCIAL INSTITUTIONS

A modern society is undeniably characterised by global ties between national and regional economic systems, and operations of banks and financial institutions play a key role in implementing this system. Business activities of these entities largely depend on safeguarding the necessary resources for regular operations, and in this sense information is perhaps even the most valuable element and thus subject to protection.

A new technological revolution brought by the process of digitalising all segments of the society, and thus also the business sphere, stresses the importance of information as a strategic resource for operations of banks and financial institutions. With no processing of data and information it would be impossible to carry out business processes, and modern business operations demand dealing with increasing amounts of information and call for their faster processing and greater availability to users, which may lead to higher vulnerability of information and threats to business operations.

Seen from the aspect of organisational and prescriptive regulation of this field, protection of information in banks and financial institutions aims to contribute to overcoming inconsistencies that occur in the practical implementation of the information protection function, in the sense of favouring the technical aspect of information protection problem at the expense of other, non-technical aspects. This paper presents relevant evidence of this inconsistency as it has been explored by scientific papers over the last twenty years. In addition, predominant theoretical thinking concurs that information protection involves protection of IT resources, human resources and business processes, which is yet another argument for the need to see the comprehensive picture of information protection without losing sight of the importance of IT resources and technical aspects of the problem. At the same time this raises questions about how it is possible to contribute to protection of information in other aspects. For these reasons, this paper examines organisational and prescriptive regulation of information protection in banks and financial institutions as a contribution to building more functional security systems of these entities.

The paper analyses published scientific knowledge to date concerning the field of information protection in banks and financial institutions as seen from the organisational and prescriptive points of view. Relevant chapters review the theoretical concept of information protection and give an overview of the prescriptive framework of the relevant field both nationally and internationally. Moreover, the paper emphasises the need to develop security awareness of all employees about the need to protect information, given that people, with their attitudes, knowledge and behaviour, represent the best mechanism of protection and the greatest source of threat. This is the source of the importance of organisational culture fields, and security culture in particular, for the development of information protection systems in banks and financial institutions.

Key words: information protection, security, information protection in banks and financial institutions, organisational regulation of information protection, prescriptive regulation of information protection, organisation, security culture

Scientific field: interdisciplinary, multidisciplinary and transdisciplinary studies

Narrow scientific field: security studies

UDC number:

САДРЖАЈ:

МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

1. ПРИСТУП ПРОБЛЕМУ

Не постоје никакве сумње да би у покушају описа данашњег света, па и када узмемо у обзир могуће различите углове посматрања феноменологије савремених појава, било оне економског, политичког, социјалног, техничког, технолошког, историјског, културолошког или неког другог аспекта разумевања стварности, приметили и значај које на савремени живот имају информације, информационе технологије и банке и финансијске институције – на први поглед разнородне тековине људске цивилизације.

У историји човечанства готово да не постоји технолошки проналазак који је нашао тако широку примену и у толикој мери изменио живот људи, као што је то информациона технологија. На овај начин изазване промене, односе се на начин прикупљања, складиштења, обраде и презентирања информација, при чему *информација постаје стратешки ресурс који се у постиндустријског ери може показати вредним и утицајним у мери у којој је то капитал био у индустријског ери*.[1]

Банке и финансијске институције представљају виталну функцију организовања и функционисања привреде у једној држави. Процесом глобализације, не само државних заједница, већ пре свега удруживањем светског капитала, дошло је до стварања светског финансијског система, где банке, односно банкарски систем представља основни систем функционисања људске заједнице у организационом смислу.

Недавна светска економска криза, позната и као *глобална финансијска криза* (2008), не улазећи овом приликом у феноменологију њеног настанка, најбољи је показатељ значаја који има *банкарски систем* на привреду и у крајњем - на стандард грађана, што *имплицира и стабилност самих државних заједница и политичке елите.*

Ипак, реалност је и да не постоји идилична слика о ресурсима које је човек кроз своју историју створио. Наука и технологија, чак и уметност, често су стварале своје сурогате које су људској заједници нанели огромне штете. Нису ли знања из физике и других техничких наука створила застрашујућа уружја за масовно уништење? Да ли су се биологија и медицина ставили у функцију само разумевања и продужења живота? Да ли се светски финансијски систем ставио у функцију остваривања хуманих циљева човечанства? Колико коштају храна и лекови за гладне? Има ли на планети довољно пијаће воде? Да ли се нафта и други енергенти плаћају само новцем? Да ли постоји тамна страна информационе технологије? Да ли и све што

[1] Петровић, С.: *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004, стр. 8

смо створили може у рукама злонамерних да нас пороби и обесмисли труд целих генерација?

Сложили би се са оним што је Асанж (*Julian Paul Assange*) рекао да „*свака створена тековина, уколико се не штити, може да представља оруђе у рукама злонамерних"*.[2] Полазећи од предмета овог рада и у смислу претходно наведеног, информатичка технологија и финансијске институције представљају вредности које, уколико се злоупотребе или не штите, могу да представљају оруђе управо у рукама злонамерних.

Информациона технологија као подршка или сегмент управљања рачунарским информационим системима доприноси складиштењу, обради, и безбедности послатих или примљених информација. Као што је познато информације без обзира да ли су усмене, писане, документационе или електронске, представљају важан сегмент у склопу пословања правног лица. Временски посматрано, данас више него у било које друго време кроз људску историју, информације су добиле на значају у свим сферама људског рада. У ширем смислу, информација се трансформише у изузетно важан елемент процеса управљања, система са којим је повезана. Било која информација ако није анализирана у оквиру одређеног контекста и благовремено примењена у конкретној ситуацији или стању, углавном остаје неупотребљена или безвредна. Добијене и стечене информације о некоме или нечему, тек када се анализирају и имплементирају у функционалну целину могу да добију своју праву употребну вредност .... Из тог разлога информација је постала једна врста робе, робе која има своју употребну вредност .....Претходно изнето неминовно намеће потребу заштите информација ....проблем заштите информација представља једну од битних радних и оперативних функција система обезбеђења. [3]

Овоме би додали и чињеницу да би пословање банака и финансијских институција данас било незамисливо без, не само масовне, већ доминантне употребе информатичких технологија, које у том смислу можемо посматрати као алат којим се прикупља, обрађује, складишти и користи огроман број информација, чиме се само потенцира значај (ризик) наведеног у претходном ставу.

Експанзија информационе технологије и аутоматизација пословних активности и процеса у свим сферама друштвеног живота заиста представља истински феномен данашњице, који је у савременом друштву донео безброј погодности, али је такође створио и низ проблема и ризика, како за појединце или групе, тако и за друштво у целини. Ове проблеме и ризике, од којих многи раније никада нису постојали, понекад је заиста тешко и замислити и разумети и представити. Оно што се никако не би могло доводити у сумњу је сазнање да је данашње друштво на прагу

[2] „Мобилни телефон је у ствари справа за праћење помоћу које можемо и да зовемо људе" - Асанж, Ц.: Слобода и будућност интернета, Albion Books, Beograd, 2013, стр. 49

[3] Мандић, Г.: *Безбедност корпоративних ресурса угрожених социјалним инжењерингом,* докторски рад, Факултет безбедности, Универзитет у Београду,

различитих форми зависности од рачунара, а та зависност ће се временом само ширити и појачавати. Та растућа зависност од информационе технологије условила је настајање бројних зона осетљивости и/или рањивости, са потенцијално врло озбиљним консеквенцама, које се могу потезати чак и до губитка контроле над њиховом судбином, што указује на чињеницу да друштвена заједница у све већој мери бива изложена новом феномену – осетљивости (рањивости) у информатичкој ери.[4]

Из ових разлога велико је интересовање савременика за стање (како је претходно наведено управо *зависности*) у области информационих технологија, а посебно у смислу сагледавања изложености безбедносним ризицима. Информациона безбедност је критична компонента управљања информационим системима, јер повећање безбедносних ризика доводи до огромних губитака за организације широм света (Campbellet al., 2003)....[5]

Различита су искуства и различити нивои развијености информационих технологија и са тим повезане информационе безбедности, па су, између осталих, забележене и тврдње неких домаћих стручњака да је „информацијска сигурност на ниско нивоу, да веома мали број организација има имплементирану сигурносну политику, али и да је „кривац“ за то великим делом законска регулатива, те занемаривање заштите информација од стране државе“[6]. Овај закључак, последица је истраживања о нивоу информацијске сигурности, где се износе тврдње да само 26% институција има систематизовано, али не и адекватно попуњено радно место менаџера за информацијску сигурност. Наиме, у јуну 2013. године, на стручном скупу у Привредној комори Србије о стању информационе безбедности у Републици Србији, изнете су тврдње да је оно алармантно јер не постоји организациона целина на државном нивоу која се тиме бави. „Нема дефинисане критичне инфраструктуре – шта треба бранити и са којим снагама и ресурсима, а само у току месец дана забележено је преко 1700 појава које се могу третирати као напад на сајт председника Србије, око 3800 покушаја скенирања система и између 1400 и 4500 покушаја напада на сајт Војске Србије, а до пре пар година није било никога ко је надгледао сајтове“.[7]

Истом приликом је изнета тврдња да „чак и САД, као најбезбеднија земља на свету, има потпуну спремност од потенцијалних сајбер напада од 10 одсто, око 47 процената су делимично припремљени а остатак је неспреман. Како је тада, такође,

---

[4] Петровић, С.: *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004, стр. 11

[5] Campbell, K., Gordon, L., Loeb, M. and Zhou, L.: *The economic cost of publicly announced information security breaches: empirical evidence from the stock market*, Journal of Computer Security, Vol. 11 No. 3, 2003., pp. 431-448.

[6] Ћосић Ј., Медић А.: *Информацијска сигурност, стандарди и стање у институцијама у БиХ*, Зборник радова V Научно-стручне конференције *Менаџмент и сигурност*, Хрватско друштво инжењера сигурности и Висока школа за сигурност, Чаковец 2010. године, стр. 115-123

[7] Вулић, И:*., Алармантно стање информационе безбедности у Србији*, http://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:437424-Alarmatno-stanje-informacione-bezbednosti-u-Srbiji, 21.12.2013.

наглашено „са ресурсима које Србија поседује јасно је на каквом је нивоу информациона безбедност земље".[8] „Србија је једна од пет земаља у Европи која још нема свој ЦЕРТ (енгл: *Computer Emergency Response Team – CERT*[9]), а постоје велике шансе да ускоро буде и једина, што говори у колико је лошем стању информациона безбедност у Србији."[10]

Такође, практично истовремено са писањем овог текста, неповољну оцену о стању у области заштите података[11] (у овом случају - о личности) даје и *Повереник за информације од јавног значаја и заштиту података о личности*: „Област заштите података о личности је крајње забрињавајућа и представља потенцијално извор све већих проблема када су у питању људска права".[12]

У таквом амбијенту, дакле не само посматрано у Републици Србији, чак не ни само у Региону, сведоци смо бројних (и све више) примера у пракси да је, посебно када је реч о банкарству и информационим технологијама, реч о „низу проблема и ризика".[13]

Говорећи уопштено о проблему сајбер одбране, државни секретар САД-а је у октобру месецу 2012. године изнео следеће[14]:

> „Сајбер напади могу бити тако деструктивни да по својим последицама могу личити на напад од једанестог септембра. Такав напад може парализовати

---

[8] *Ibid*

[9] више о ЦЕРТ-у, као и о Агенцији европске уније за безбедност мрежа и података (енгл: *the European Union Agency for Network and Information Security* – ***ENISA***) биће даље у раду

[10] Вулић, И., *Ibid*

[11] Појмовно разграничење термина „податак" и „информација" даћемо на другом месту, посебно јер у смислу изнетог ова разлика није од значаја

[12] http://www.blic.rs/Vesti/Drustvo/426048/Sabic-Zabrinjavajuce-stanje-u-oblasti-zastite-podataka, 21.12.2013.

[13] У САД су 2009. године ухапшене три особе осумњичене да су проучавајући податке успешних компанија дошле до више од 130 милиона бројева кредитних и платних картица које су намеравали да продају на нелегалном тржишту: http://www.rts.rs/page/stories/sr/story/10/Svet/99601/Najve%C4%87a+kra%C4%91a+identiteta+u+SAD.html, 15.12.2013. У Енглеској је 2013. године ухапшено осам особа (мушкарци старости од 24 до 27 година) због крађе два милиона долара, тако што су неовлашћено приступили информационом систему једне банке (Баркли банка). Ухваћени су када је један од њих покушао да као лажни инжењер у шпанској банци Сантандер инсталира „миш" који је требао да им омогући контролу над информационим системом Банке: http://www.24sata.rs/vesti/svet/vest/osmoro-uhapseno-zbog-sajber-pljacke-banke/106458.phtml, 15.12.2013.

У Републици Србији, 2013. године, ухапшена је особа која једну банку оштетила за близу један милион Евра, тако што се у периоду од око месеца дана, подизања новца на рачуну извршиоца приказивало као приход на том истом рачуну. „Грешка" се догодила у тренутку када је у банци дошло до примене новог софтвера који је и служио за контролу платних картица и њихову ауторизацију. http://www.pressonline.rs/info/hronika/291744/opljackao-banku-za-milion-evra-dizuci-novac-sa-svog-racuna.html, 15.12.2013.

[14] http://media.bloomberg.com/bb/avfile/rjrab4Iz4sfg, 21.12.2013.

нацију. У последњих неколико недеља, неке велике америчке финансијске институције су погођене таквим сајбер нападима да су њихови интернет сервиси били привремено недоступни. Постоје и еклатантнији примери оваквих напада, као што је софистицирани вирус који је напао рачунаре нафтне компаније у Саудисјкој Арабији, када су датотеке замењене фотографијом запаљене америчке заставе. Тридесет хиљада рачунара је тада морало да буде замењено. Само неколико дана након овог инцидента био је напад на главну гасну компанију у том региону (у Катару). Ми знамо да страни сајбер актери сондирају мрежу америчке критичне инфраструктуре. Тако се могу напасти контролни рачунари који контролишу хемијску или енергетску индустрију или водовод. Нападач би могао да настоји да, на пример, избаци из колосека возове са смртоносним товаром који би даље могао да контаминира воду за снабдевање у великим градовима...Најдеструктивнија сценарија укључују могућности неколико истовремених напада на критичну инфраструктуру, у комбинацији са физичким нападом на земљу. Резултат ових врста напада може бити „сајбер перл Харбор“, напад који би изазвао паралисање нације и који би створио осећај свеопште угрожености. Као директор ЦИА-а, а сада Секретар одбране, знам да су сајбер претње подједнако реалне као оне које су нам већ познате“....“Министарство одбране је зато развило софистицирани систем за детекцију сајбер уљеза, а ангажовани су и сви други безбедносни ресурси, који су фокусирани на ову безбедносну претњу и који настоје да створе сигуран сајбер простор“...“то не значи да ћемо због тога пратити личне рачунаре грађана – то није наша мисија...“...“у прошлости , ми смо тако радили преко операција на копну, мору и на небу. У овом веку САД војска мора да брани народ помоћу одбране од сајбер спејс простора“...“Да би се обезбедило да испунимо нашу улогу у сајбер простору посветићемо се пре свега на: (1) развој нових способности, (2) успостављање одговарајуће политике и организације и (3) изградњу ефикасне сарадње са индустријама и међународним партнерима.”

У трци са технологијом многи постојећи системи са онлајн услугама имају мање него задовољавајућу контролу обезбеђења .Такви системи врше функције као што су берзанска и банкарска пословања, контрола нуклеарног наоружања, вођење и контрола ваздушног саобраћаја, хитнс службе. Владе почињу да препознају недостатке таквих система и дефинисале су потребу за бољим степеном заштите. Критичним тачкама система је означено следећих пет области:[15]

- информатика и комуникације;

[15] Ранђеловић Д.: *Високотехнолошки криминал*, Криминалистичко-полицијска академија, Београд 2013, стр. 275

- *банкарство и финансије;*
- енергија (нафта, гас, струја);
- достава трговинских производа;
- услуге од виталног значаја за човека.

Полазећи од до сада наведеног, намеће се закључак да област заштите информација у банкама и финансијским институцијама, јесте део актуелног и глобалног проблема заштите информација, а специфичност нашег предмета истраживања огледа се управо у значају који на живот савременог човека имају саме финансијске институције, услед чега можемо да тврдимо да је овде реч о двострукој неопходности и актуелности оваквих научних разматрања.

2. ПРЕДМЕТ ИСТРАЖИВАЊА

Предмет истраживања је заштита информација у банкама и финансијским институцијама, првенствено полазећи од организационог и нормативног аспекта уређења и обављања ових послова. Два су основана разлога за овакав одабир предмета истраживања: са једне стране опажамо несумњив значај који имају нормативна уређеност и организација као претпоставке успешног функцинисања пословних функција, а посебно безбедносне пословне функције, док са друге стране видимо извесно и, наше је мишљење, неоправдано поистовећивање целокупне области заштите информација − што би била информациона безбедност (енгл: *Information Security - IS*) са информатичком заштитом − односно информатичком безбедношћу (engl: *IT security*) – што у крајњем може да имплицира измену целокупног концепта система безбедности, у смислу занемаривања традиционалних сегмената система безбедности − физичке безбедности (енгл: *Physical Security – PS*) за рачун, информационе безбедности чиме се даље последично долази до конституисања некомплетног система безбедности, посебно у смислу његове неравномерне функционалне развијености и неефикасности у пракси.

У раду ћемо настојати да сагледамо објективне потребе у остваривању безбедности информација у банкама и финансијским институцијама, које диктира безбедносно окружење, прихватајући при томе не само одговарајуће ризике већ и имајући у виду нарочито нормативне и организационе механизме које савремено друштво већ успоставља у вечитом стремљењу одбране од свих врста опасности, па тиме и у одбрани од опасности које долазе из информационе сфере.

Научни приступ у конципирању система безбедности, уколико на овом месту себи дозволимо високи ниво уопштавања, подразумева и неселективно разматрање *свих извора угрожавања* (последично и свих облика супротсављања). У области заштите информација, то подразумева пре свега безбедносну свест, а затим и прихватање, специфичности које са собом носе технолошка знања и достигнућа у

сфери информационих технологија, али и потреба да се овом проблему приступи систематично, одакле се, наша је претпоставка, информационе технологије могу посматрати (само) као средство у постизању циљева система безбедности, а не као универзални чинилац или извориште, средство и циљ информационе заштите, од којег не видимо било које друге аспекте безбедносног организовања (па тако на пример ни организационог а ни нормативног уређења заштите информација).[16]

Заштита података јесте широко обрађивана тема у научним радовима последњих деценија, но конкретно усмерена ка банкама и финансијским установама, са посебним освртом на организационо и нормативно уређење, ипак није тако често истраживана тема па је, с тим у вези, била изазов. Слична ствар је и у Републици Србији, ретки су научни радови који се уопште баве информационом безбедношћу а посебно њеним специфичностима. Ипак у једном од њих се упућује на ширину поља деловања у предметној области, у смислу како и ми видимо научни приступ проблему заштите података у банкама и финансијским установама, па тако аутор Ранђеловић наводи: „Кибер криминал[17] је суштински класичан криминал извршен у информационом амбијенту“...“Сваким даном се, развојем информационих технологија и тиме амбијента појављују нове врсте злоупотреба. Сама чињеница да се све те врсте криминала извршавају у амбијенту у којем информационе технологије имају доминантну улогу, подразумева присутност одређених специфичности у односу на класичан криминал...“[18]. Тако овај аутор, на истом месту, даје *преглед врста злоупотреба у сајбер криминалу* и тим поводом таксативно наводи, којом приликом је назначио да је тај скуп није коначан, да су то: крађе, преваре, проневере, фалсификовање, изнуде, уцене, нарушавање приватности, саботажа, одавање тајне, шпијунажа, порнографија, пропаганда, вандализам, тероризам и убиства. Уз ове облике криминала он додаје и *облике који представљају посебност „кибер криминала*“, а то су: хаковање, стварање и дистрибуција вируса, пиратство софтвера, ускраћивање сервисних услуга, електронско узнемиравање и крађа рачунарских услуга.

У будућности, рапидно ће се повећати обим и фреквенција сајбер криминала због исто тако рапидног повећања броја рачунара, аутоматизације пословних активности и процеса, интеграције рачунарских мрежа, снижења доњег прага знања и стручности потребних за коришћење информационе технологије и ширења

[16] Тако је Народна банка Србије донела *Одлуку о минималним стандардима управљања информационом системом финансијске институције,* Службени гласник РС, бр. 23/2013, где се препознаје проблем безбедности на начин како смо ми навели у тексу: „ Овом Одлуком утврђују се минимални стандарди и услови стабилног и сигурног пословања који се односе на управљање информационим системом банака..“, Члан 1.

[17] за потребе овог рада ми ћемо користити друге термине, о чему ће бити речи даље у тексу, а посебно у делу теоријског одређења предмета истраживања

[18] Ранђеловић Д.: *Високотехнолошки криминал*, Криминалистичко-полицијска академија, Београд, 2013., стр. 260

компјутерске писмености, која већ сада постаје главна одредница времена у којем живимо.[19]

На овом месту ми би подсетили да је овим прогнозама, које долазе првенствено из сајбер простора, што је у литератури уобичајено када се говори о претњама у *заштити информација* банака и финансијских институција, дакле уобичајено, али не и оправдано како ми истичемо, потребно додати и разматрање шта ће се догодити са трендовима других облика претњи (класичне крађе, преваре природне непогоде, индустријска шпијунажа и друго[20]).

3. ТЕОРИЈСКИ И КОНЦЕПТУАЛНИ ОКВИР ИСТРАЖИВАЊА

Тема која је изабрана за предмет истраживања у основи захтева теоријско и концептуално разграничење информационе и сајбер безбедности које су дефиницијски веома сличне, али, према неким ауторима, даје се већа концептуална ширина сајбер безбедности која, између осталог, укључује људе са њиховим личним својствима и друштво у целини, при чему могу бити директно оштећени или погођени сајбер нападима, док то није случај са информационом безбедношћу где штета може бити индиректна (Solms, Niekerk, 2013). Сајбер безбедност је питање глобалног интереса и важности и највећи део нација данас је објавио неки облик стратешког документа у коме се износе и званични ставови о сајбер простору, сајбер криминалу и/или сајбер безбедности. Оно што је уочено, то је да се у мањем броју извора прави разлика између сајбер безбедности и информационе безбедности или односа између њих. Овде можемо издвојити дефиницију сајбер безбедности коју је дала Међународна унија за телекомуникације у којој се каже:

> „Сајбер безбедност је колекција алата, политика, безбедносних концепата, безбедносних мера заштите, смерница, приступа управљању ризиком, акција, обука, најбољих пракси, осигурања и технологија које се могу користити за заштиту сајбер окружења и организација и имовина корисника. Средства организације и корисника укључују повезане рачунарске уређаје, особље, инфраструктуру, апликације, услуге, телекомуникационе системе и укупност послатих и/или усклађених информација у сајбер окружењу. Сајбер безбедност настоји осигурати постизање и одржавање безбедносних својстава организације и корисничких средстава у односу на релевантне

[19] *Ibid*

[20] Сајбер тероризам је можда карактеристичан у том смислу, јер и ако користи сајбер простор да би се остварио као претња, он није само сајбер проблем и не решава се само информатичким ресурсима. Претходно смо у тексу навели гледање америчког државног секретара за одбрану, који у том смислу наводи да се реалне претње сајбер терориста да путем информатичких ресурса изазову индустријске, саобраћајне, придодне и друге катастрофе

безбедносне ризике у сајбер окружењу. Општи безбедносни циљеви обухватају следеће:доступност, интегритет, поверљивост“

(ITU, 2008).

На сличан начин је и Европска мрежа и агенција за информациону безбедност (ENISA) дефинисала сајбер безбедност као „збирка алата, политика, концепата, безбедносних мера, смерница, обука, најбоље праксе и технологија које се могу користити за заштиту сајбер простора и имовине корисника.

Ако погледамо дефиницију информационе безбедности, она се може објаснити на више начина, па тако Међународни стандард ИСО /ИЕЦ 27002 (2005) дефинише је као „очување поверљивости, интегритета и доступности информација“, при чему информације могу да попримају различите форме, могу се штампати, написати на папиру, чувати електронским путем, преносити поштом или електронским путем, приказати на филмовима, пренети усмено у разговору и на много других начина. Витман и Маторд дефинишу информациону безбедност као „ заштита информација и њених критичних елемената, укључујући системе и хардвер који користе, складиште и преносе те информације“. Ови аутори такође, идентификују неколико критичних карактеристика информационе безбедности које јој дају вредност у организацијама, а оне укључују поверљивост, интегритет и доступност информација, као и дефиниција ИСО стандарда, али поред њих укључују и обезбеђивање поверљивости, интегритета и доступности информација које су познате као ЦИА троугао, што је традиционално индустријски стандард. Циљ информационе безбедности је осигурање континуитета пословања и минимизирање пословне штете ограничавањем утицаја безбедносних инцидената. Многи аутори се слажу да информациона безбедност није производ или технологија, чак ни само техничко питање, већ процес. Наиме, процес заштите рачунара и мрежа се временом тако развијао да је превазишао техничка питања, која су почетно преовладавала.[21] У складу са овим, потребно је правити разлику између информационе безбедности и информационе технологије или информационе и комуникационе технологије.

Извесна нејасноћа у разликовању, досада наведених појмова, заправо доприноси заједничком пољу знања из области информационе и сајбер безбедности, јер такав скуп знања пружа „основу за разумевање термина и појмова“ у предметној области и тако делује као „таксономија тема релевантних за професионалце широм света,“[22] што ће рећи, класификацију ствари или концепата, као и принципе на којима се темељи таква класификација.

Комплексност теоријског и концептуалног одређења кључних појмова се карактерише и чињеницом да не постоји теоријска усаглашеност око самог појма

[21] Видети: Mitnick K, Simon W.: *The art of deception: controlling the human element of security,* Wiley Publishing; 2002.

[22] Theoharidou M. Gritzalis, D.: *Common body of knowledge for information security,* Security & privacy, IEEE, Видети: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber¼4140992; 2007.

безбедности, па тиме ни појмова који извиру из овог појмовног одређења, али и чињеницом да област заштите информација, како смо претходно навели, карактерише широк дијапазон појмова који се у литератури смењују у истраживачком пољу и доминацији коју наизменично остварују. Дакле, то су примери наизменичне употребе појмова информационе, рачунарске, кибер, сајбер, безбедности и други, одакле овде, последично, као једна од карактеристика саме информатике као научне области, влада масовно преузимање појмова који су на глобалном нивоу опште прихваћени, са често основаним образложењем да су неки од појмова тешко преводиви (софтвер, хардвер, бекап, логовање, редудантност, интернет, ПИН код, пасворд, итд.).

Уважавајући управо навођење значаја обезбеђивања поверљивости, интегритета и доступности информација уочава се и важност других елемената који излазе из сфере техничког. Наиме, у докторском раду *Mark A. Harris,* истражује проблем одређивања програмског садржаја у безбедносним обукама, првенствено у области развоја безбедносне свести (енгл: *Security Awareness*). Аутор истиче значај обуке у области заштите информација, али истовремено примећује да су безбедосне политике, обуке и сам кадар који обавља ове послове неоправдано често (само) техничке природе, те да је последица оваквог стања занемаривање других приступа (погледа), посебно погледа из угла друштвеног аспекта овог проблема.[23]

На истом месту се наводи да су постојала и ранија истраживања која су доказала претпоставку да је у области заштите информација најцелисходније имати такав приступ који се базира на знањима и друштвених и техничких наука (Backhouse & Dhillon, 1996; Dhillon and Backhouse, 2000, 2001; Trompeter & Eloff, 2001; Siponen, 2001; Dhillon & Torkzadeh, 2006; Dhillon, 2007). [24]

Такође, савремена истраживања указују да се у безбедносним политикама заштите информација запоставља друштвени карактер ових феномена (Rotvold, 2008; CWS, 2010; Fulford & Doherty, 2003).

Полазећи од предмета истраживања, потребно је одредити значење више кључних поојмова, којом приликом на овом месту немамо амбицију да их све таксативно наведемо, већ ће се они дискутовати у тексту како се буду појављивали у нашим даљим разматрањима.

Комплексност теоријског одређења кључних појмова се карактерише двема чињеницама: не постоји теоријска усаглашеност око самог појма безбедности, па тиме ни појмова који извиру из овог појмовног одређења и - област заштите информација, како смо претходно навели, карактерише доминација информационе („рачунарске“, „кибер“, „сајбер“, итд.) безбедности, одакле овде, последично, као једна од карактеристика саме информатике као научне области, влада масовно преузимање појмова који су на глобалном нивоу опште прихваћени, са често основаним

[23] Mark A Harris: *The shaping of manager's security objectives through information security awareness training,* PhD dissertation, Virginia Commonwealth University, 2010
[24] *Ibid*

образложењем да су неки од појмова тешко преводиви (софтвер, хардвер, бекап, логовање, редудантност, интернет, ПИН код, пасворд, итд.).

Коришћење термина који долазе из другог језика, њихово преузимање за потребе коришћења српског језика, можемо да критикујемо са више аспеката – у негативној конотацији. Ипак, овакав приступ, истовремено може да поседује и практичну предност када је у питању разумевање неких појмова – посебно на нивоу једне професије (па тако можемо говорити о језику професије у информационим технологијама (енгл: *Information Tehnology – IT*) – у *IT* технологијама). Из тих разлога, повремено ћемо се у тексту служити терминима који очигледно долазе из енглеског језика, али је њихова примена толико масовно прихваћена да коришћење ових термина не изазива недоумицу у погледу опсега неког појма.[25]

Када се говори о информационој безбедности морамо увести у разматрање или барем на основном нивоу појаснити и друге сродне појмове или појмове који гравитирају једни ка другима у очигледно широкој области која повезује информације, безбедност, заштиту и тсл.

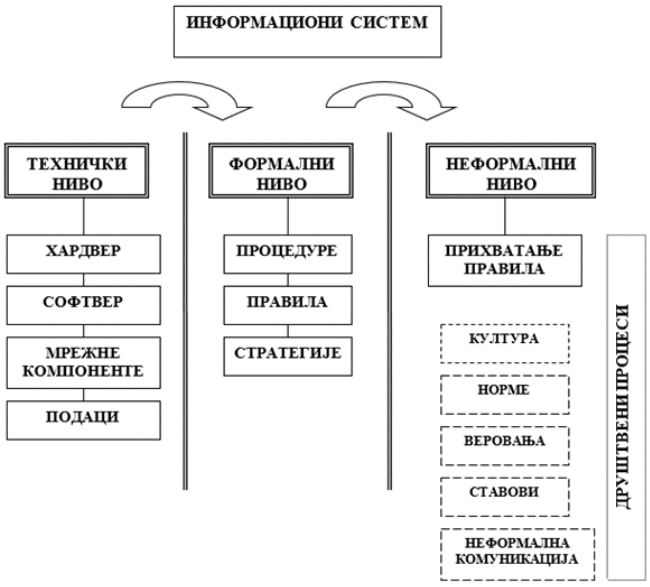
Информациои систем (безбедности), како наводи *Dhillon* (2007)[26] је систем који обрађује информације на три нивоа: техничком, формалном и неформалном нивоу[27]. Софтвер, хардвер, подаци и мрежне компоненте чине технички ниво. То је све оно што подржава проток и обраду информација. Формални ниво подразумева правила и процедуре (као што су безбедносне стратегије, политике и процеси). Прихватање правила формалног система од стране људи је друштвени процес, који је део неформалног система, којег такође сачињавају и култура, норме, веровања, ставови и неформална комуникација. Дилон инсистира на координацији између ова три система и том приликом користи аналогију са прженим јајетом. Жуманце представља технички систем, формални систем представља опну између жуманцета и беланцета, које представља неформални део информационог система. Аутор истиче значај неформалног система и, у смислу аналогије коју је дао, техничком делу додељује подређену улогу. Такође Дилан упозорава и на важност „преформализације“ формалног дела и значаја који он има у односу са неформалним делом система.[28]

Слично томе, *Политика безбедности* Информационог система[29] укључује намере и приоритете у погледу заштите *IS*, што можемо назвати и циљевима безбедности, заједно са општим описом средстава и метода које су потребне за постизање тих циљева. Ови циљеви су апстрактни у природи и написани су у општим

[25] Тако, искуствено опажамо да можемо, на пример, дискутовати на српском језику о значењу термина „безбедност“ и „заштита“, али ако говоримо у окружењу професионалаца и припадинка академске заједнице из света безбедности, о терминима из енглескоj језика „*security*“ и „*safety*“, потреба за таквом дискусијом, због јасне терминолошке одређености, одједном ће престати!
[26] *Ibid,* str. 9
[27] Dhillon, Gurpreet: *Principles of Information Systems Security: Text and Cases*, John Wiley & Sons, 2007
[28] *Ibid,* str. 5
[29] *Ibid,* str. 9

терминима. Пример за то могу бити изјаве о потреби да се заштите осетљиви подаци од неовлашћеног приступа. На нижем нивоу, процедурално се одређује на који начин се постижу (претходно) прокламовани циљеви (одговарајућим политикама) информационе безбедности (Схема број 1: *Нивои информационог система према Дилану*).

Схема број 1: *Нивои информационог система према Дилану*



Тренинг у области безбедности информација (енгл: *Information security Training*), или како се у енглеском говорном подручју често говори развој безбедносне свести (енгл: *Security Awareness*) је метод образовања свих запослених о томе како најбоље да заштите информациони систем организације. Најшешће обука одражава процедурално оријентисану безбедносну политику. Са друге стране, најефикаснији безбедносни тренинг би третирао претње и са техничког и са друштеног аспекта.[30]

У раду који истражује понашање запослених у смислу усклађености њиховог понашања са безбедносном политиком заштите информација[31], аутори износе тврдње да су запослени највећа претња заштити информација, и да је у остваривању ове заштите најважнији квалитет информација које запослени имају, те да се поред свести о опасностима угрожавања безбедности информација мора радити на постизању усаглашености вредности које запослени имају са прокламованим вредностима (у безбедосним политикама).

[30] *Ibid*, str. 11

[31] Seppo Pahnilaa, Mikko Siponena and Adam Mahmood: *Employees' Behavior towards IS Security Policy Compliance*, 40th Hawaii International Conference on System Sciences - 2007

Сајбер безбедност (енгл: Cybersecurity[32]):

Сајбер безбедност је збирка алата, политика, концепата, безбедносних мера, смерница, обука, најбоље праксе и технологија које се могу користити за заштиту сајбер простора и имовине корисинка.

Сајбер криминал (енгл: Cybercrime[33]):

Сајбер криминал покрива широк спектар криминалних активности, услед чега је тешко дати јединствену дефиницију. Рачунари, у овом смислу, могу бити истовремено и средство и циљ. На интернету, време и место злочина немају исти смисао као што је то у физичком свету. То се најбоље види на примеру „фишинга" (енгл: *phishing*)[34], јер се новац може украсти са банковног рачуна на различитим местима у свету и у било којем тренутку, одакле овакво дело може бити начињено у различитим правним системима, што даље отежава пут правде (тужилаштво једне земље настоји да лиши слободе лице у некој другој земљи). Наравно да ово посебно погодује организованом и високо технолошком криминалу.

Сајбер шпијунажа (енгл: Cyber espionage[35]): представља добијање осетљиве (поверљиве) информације користећи нелегалне методе експлоатације на интернету. Европски извештај *ENISA*-е за 2012. годину, је навео да су на Блиском истоку рачунари у неколико земаља дизајнирани тако да „прислушкују" финансијске трансакције, те да је Касперски тим у Русији (енгл: *Kaspersky*) открио вирус који има сврху надзора над рачунарима у Либану и другим земљама у том региону.[36]

---

[32] *EU cyber cooperation: the digital frontline,* European Network and Information Security Agency (ENISA), 2012, доступно на: https://www.enisa.europa.eu/publications/eu-cyber-cooperation-the-digital-frontline/

[33] *Ibid*

[34] Реч је о облику сајбер криминала који је заснован на методама социјалног инжењеринга. Суштина је у навођењу корисника на лажну интернет стварницу где се кориснику захтева, из различитих „добронамерних" разлога да се поново представи својом шифром (бројем кредитне картице, PIN-ом и слично), одакле она постаје позната злонамерним особама и касније употребљена за (најчешће) крађу новца са банковног рачуна.

[35] *Ibid*

[36] Реч је о вирусу koji је назван „Гаус" (енгл: *Gauss*). Касперски тврди да су овај вирус направили исти они који су направили и , раније већ познате, *Stuxnet* и *Flame* вирусе. *Stuxnet* је наводно, према његовим речима, направљен од стране САД и Израела, како би се омео рад Иранског нуклеарног постројења. *Flame* је у току 2012. године у земљама Блиског истока био инсталиран да снима комуникацију, укључујући *Skype* позиве и друге мрежне активности и да краде фајлове и да их шаље нападачу. Када су антивирусне компаније почеле да истражују овај вирус, послата је команда која је уништила све инкарнације овог вируса (енгл: *malwer*-а) и он је нетрагом нестао. Касперски такође тврди да су за развој оваквих вируса (поред споменутиих ту убраја и вирус под називом Црвени октобар, енгл: *Red October*) потребни буџети од више десетина милиона долара, као и да сајбер криминал није толики проблем колико су то управо сајбер шпијунажа и напад на критичну инфраструктуру. Види:

Сајбер ратовање (енгл: Cyber warfare): представља ратовање у сајбер простору средствима информационе технологије. Мета је критична инфраструктура.[37]

Безбедност: изведена из латинског језика *securitas,* енглеска реч *„security"* значи осећај или стање слободе од претње уништењем. Под овим појмом се подразумева: *стање безбедности, средства за постизање безбедности* и *осећај безбедности*[38]. Много је дефиниција безбедности јер је, како су се многи аутори сложили, вишедимензионална и у концептуалном смислу и у практичном, а њена права природа се може разумети и сагледати тек из контекстуалне перспективе.Тако се безбедност може дефинисати као „стабилно, релативно предвидљиво окружење у којем појединац или група могу стремити својим циљевима без поремећаја или штете и без страха од таквих поремећаја или повреда"[39] или, у нешто традиционалнијем смислу: „ пружање приватних услуга у заштити људи, информација и средстава за појединачну сигурност или добробит у заједници" Поред тога кроз оквир приватног или комерцијалног обезбеђења може се посматрати као пружање плаћених услуга у спречавању нежељених, неовлашћених или штетних губитака имовине организације.[40] И наравно, у свом знатно ширем оквиру безбедност се везује за контекст националне безбедности и одбране. Можемо још једном поновити и наглашавање разлике између појмова безбедности и сигурности или заштите, што је додатни нагласак на заштиту од опасности које потичу споља. Безбедносна претња или ризик је неко или нешто што намерава или би могло нанети штету, примењено споља (идеја спољне претње се не треба схватити дословно). Сигурност се фокусира на процес у унутрашњем окружењу и сматра се да је безбедносне претње и ризике, за разлику од сигурносних, далеко теже решити, јер ће нападач покушати да искористи своју људску домишљатост да заобиђе било који систем заштите.

Нормативно уређење: **у** свету правна регулатива из обалсти *компјутерског криминала* датира од 1973. године, када је у Шведској донет пропис који познаје кривично правну заштиту од компјутерског криминалитета, а од тада су слично поступиле многе државе. Република Србија је потписала 23. новембра 2001. године Конвенцију о високотехнолошком криминалу[41]. У овој области врло је активна међународна сарадња (јер ни ризици који долазе из сајбер сфере нису локалног, односно националног карактера), тако да најбројније активности креирају Организација

http://www.informacija.rs/Vesti/Stuxnet-je-zarazio-i-jednu-rusku-nuklearnu-elektranu-tvrdi-direktor-Kaspersky-Lab-a-VIDEO.html 25.12.2013.

[37] Види фус ноту број 13

[38] Детаљније о термину *security* у: Бајагић М.: Основи безбедности, Криминалистичко-полицијска академија, Београд, 2007., стр. 11

[39] Fischer, R.J., Halibozek, E., Green, G.: *Introduction to Security*, eighth ed. Butterworth-Heinemann, Boston, 2008.

[40] Post, R.S., Kingsbury, A.A.: *Security Administration: An Introduction to the Protection Services*, fourth ed. Butterworth-Heinemann, Boston, 1991.

[41] Ранђеловић Д.: *Високотехнолошки криминал*, Криминалистичко-полицијска академија, 2013., стр. 309

уједињених нација, Организација за европску сарадњу и развој (ОЕЦД), Савет Европе и Европска унија – о чему ће детаљније бити излагано даље у тексту овог рада. Област сузбијања компјутерског криминала је у Републици Србији уређена међународним конвенцијама, законским и подзаконским актима, и то:

- Закон о потврђивању конвенције о високотехнолошком криминалу, *Службени гласник РС – Међународни уговори*, бр. 19/2009
- Међународна конвенција о заштити извођача, произвођача фонограма и установа за радио дифузију од 26. октобра 1961. године, потврђена Законом о потврђивању међународне конвенције о заштити извођача, произвођача фонограма и установа за радио дифузију, *Службени лист СРЈ – Међународни уговор*, бр. 13/2002.
- Уредба о ратификацији париске конвенције о заштити индустријске својине, *Службени лист СРЈ – Међународни уговор*, бр. 5/74 и 7/86
- Уредба о ратификацији Светске конвенције о ауторском праву, *Службени лист СФРЈ – Међународни уговори и други споразуми*, бр. 4/66 и 54/73.
- Директива Савета (ЕЕЗ) о правно јзаштити рачунарских програма, бр. 61/250 од 14. маја 1991., *Службени лист ЕЗ*, бр. Л 122, 17. мај 1991.
- Директива Европског парламента и савета (ЕЕЗ) о правној заштити база података бр. 96/9, 11. март 1996.
- Кривични законик Републике Србије (Службени гласник РС, бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009 и 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019)
- Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, бр. 61/2005 и 104/2009
- бројни други прописи који на различитом ниову регулишу ову област, а који ће у завнисности од потребе бити наведени даље у тексту

Од значаја је напоменути, када је у питању правна регулатива, да су у домаћем законодавству дефинисана и *кривична дела из области компјутерског криминала*, па је тако у глави XXVII КЗ наведено:

- оштећење рачунарских података и програма
- рачунарска саботажа
- прављење и уношење рачунарских вируса
- рачунарска превара
- неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података
- спречавање и ограничавање приступа јавној рачунарској мрежи

– неовлашћено коришћење рачунара или рачунарске мреже

– прављење, набављање и давање другом средства за извршење кривичних дела против безбедности рачунарских података

Рачунарски податак: рачунарски податак је свако представљање чињеница, информација или концепата, у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу којег рачунарски систем обавља своју функцију. [42]

Изменама и допунама КЗ, длеима у вези са злоупотребом рачунарске технологије обухваћена су и дела дечје порнографије и *злоупотребе платних картица*, за које су запрећене казне затвора од пет до осам година.

Према одредбама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала у РС, исти је дифинисан као вршење кривичних дела код којих се као објекат или средство извршења кривичних дела појављују рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.[43]

Информација: у свим областима свог деловања човек свесно своју активност усмерава ка циљу који жели да достигне користећи се разним врстама сазнања. Анализом постојећег сазнања - податка и његовим употребом податак добија нову квалитативну вредност и постаје *информација*. С обзиром да постоје различите дефиниције појма информације, за даље разматрање овог појма као полазну основу можемо узети две дефиниције које по свом садржају одговарају потребама даљег излагања. Информација је функција односа између могућих одговора пре и после пријема поруке (Луј-Марсел Бриљон, 1854-1948), и информација је назив за садржај који је размењен са спољашњим светом у поступку усаглашавања са њим (Норберт Винер 1894-1964).[44] Можемо рећи и да је то „знање добијено истрагом, проучавањем или упутством“ како стоји у Вебстеровом речнику, или да се вратимо теорији информација која је формулисана како би се решио одређени специфични технолошки проблем и која је опет везана за концепт знања, па се информација може мерити као „разлика између стања знања примаоца пре и након преношења информација.“[45]

Банке и финансијске институције: банка се може сматрати пословном јединицом (предузећем) која обезбеђује банкарске производе у профитне сврхе. У зависности од различитих услова у којима се банкарство развијало у појединим земљама, јавиле су се и разне дефиниције банака. У Енглеској се сматра да је основна карактеристика банака новчана емисија, у Француској је посредовање у одобравању кредита, док је у Немачкој

[42] *Ibid,* Глава XII KZ

[43] *Ibid*

[44] Цигурски, О.: *Информатика*, Факултет цивилне одбране, Београд, 2002., стр. 41.

[45] Bell, D.A.: *Information Theory and its Engineering Applications*. London: Pitman & Sons. 1957.

њихово учешће на берзама и вабљење новчаним шпекулацијама. Банка је новчано предузеће и кредитна установа чија је основна активност депозитни посао, узимање и давање кредита, посредовање у области кредита и обављање других новчаних послова за рачун својих клијената.[46]

Организовање се врши у циљу управљања предузећем или неким другим обликом организације. Из тог разлога, организовање се сматра једном од фаза процеса управљања. Менаџмент се дефинише као процес планирања, организовања, вођења и контроле напора чланова организације и осталих ресурса ради остваривања циљева организације.

Сва истраживања организације као и радови који су из њих резултирали могу се поделити у три велике области: [47]

Организациона теорија и дизајн: овај сегмент организације има за предмет проучавања структуралне, формалне или, како се то у жаргону каже *„hard“,* елементе организације. Основне теме интересовања у овој области организације су: организациона структура и системи. Они су формалне природе у смислу да су готово увек формално санкционисани одлукама управе организације. Теме истраживања у овој области су: подела рада, дистрибуција ауторитета доношења одлука, груписање јединица, број хијерархијских нивоа, распон контроле руководиоца, координација....циљ је открити факторе од којих зависи обликовање структуралних компоненти организационог дизајна. Најзад, циљ истраживања јесте и моделирање структуре и система организације како би се у одређеним типичним ситуацијама применили одговарајући модели

Организационо понашање или понашање људи у организацији: фокус истраживања у овој области јесте човек. Два су основна задатка истраживача у организационом понашању: објаснити понашање људи у организацијама и открити начин на који се на њега може утицати.

Организационе промене и развој: има за предмет интересовања промене организације. Основни истраживачки задатак ове области јесте открити како изводити промене организације.

Полазећи од предмета истраживања овог рада, ми ћемо посебну пажњу посветити аспектима које, према наведеном, подразумева организациона теорије и дизајн, будући да нас интересује на који је начин организована заштита информација у банкама, те који су њени механизми остваривања у конкретним срединама. Да би то постигли, морамо упознати њене хијерархијске нивое на којима је успостављена као пословна функција, како се обавља контрола спповођења заштите информација и друго.

[46] Хаџић М.: Банкарство, Факултет за финансијски менаџмент и банкарство, Београд, 2007., стр. 11
[47] Петковић М., Јанићијевић Н., Богићевић Б.: Организација , Економски факултет, Београд 2002., стр. 15.

Сматрамо, и ако се ми нећемо посебно задржавати на њој, да је од нарочитог значаја, посебно за евентуална будућа истраживања из предметне области, слика која би се добила посматрајући проблем са аспекта Организационог понашања. Ово из разлога јер смо, а све у циљу изградње успешног модела заштите информација у банакама и финансијским институцијама, врло заинтересовани за проблемске области које се односе на: мотивацију (на пример: мотивисаност запослених да усвоје, примењују и промовишу безбедносну политику организације), организационо учење, преговарање, управљање конфликтима, организациону културу и друго. На овом месту, рекли би само да сматрамо да је значајна свест коју запослени имају о потреби заштите информација, односно сматрамо да је безбедносна свест значајан део организационе културе.

4. ОПЕРАЦИОНАЛНО ОДРЕЂЕЊЕ ПРЕДМЕТА ИСТРАЖИВАЊА

Операционо одређење предмета истраживања планирали смо кроз реализацију неколико истраживачких етапа и то:

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

Друга фаза односи се на анализу постојећег нормативног оквира који се бави питањем заштите информација,

У *трећој фази* планирамо да спроведемо емпиријско истраживање са циљем утврђивања постојећег стања у области заштите информација у банкама и финансијским установама у Републици Србији.

Коначно, планирамо да претходно утврђени нормативни оквир, као и форму организације, упоредимо са добијеним резултатима истраживања и да на основу анализе садржаја сагледамо правце развоја система заштите информација у банкама - у контексту боље фукционализације целокупног безбедносног система у овим субјектима.

5. ВРЕМЕНСКО, ПРОСТОРНО И ДИСЦИПЛИНАРНО ОДРЕЂЕЊЕ

5.1. Временско одређење

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

Анкетна истраживања, планирамо да спроведемо у току прве половине 2015. године.

5.2. Просторно одређење

Предмет истраживања је првобитно замишљен да буде просторно ограничен на подручје Републике Србије – нарочито у делу који се тиче анкетног истраживања (у међувремену се одустало). Теоријска истраживања и анализа садржаја, полазећи од чињенице ширине сајбер простора, обухватиће савремене трендове у области система заштите информација у банкама и финансијским институцијама, дакле знатно шири простор – не ограничавајући се на конкретне регије.

5.3. Дисциплинарно одређење

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

6. ЦИЉ ИСТРАЖИВАЊА

Истраживање има за општи циљ да утврди резултате анализе заштите информација у банкама и финансијским институцијама, са аспекта организационе и нормативне уређености.

Значај истраживања ће се испољити у проналажењу научно верификованих теоријских и емпиријских сазнања о специфичностима система заштите информација у банкама и финансијским установама и предузимању потребних мера.

6.1. Научни циљ истраживања

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

6.2. Практични циљеви истраживања

Резултати теоријског и емпиријског истраживања могу представљати ваљан основ за даљу праксу у заштити информација у банкама и финансијским установама.

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

7. ХИПОТЕТИЧКИ ОКВИР

Заштита информација у банкама и финансијским институцијама у пракси се базира се на информационој (*IT*) безбедности, чиме се имплицира развој других неопходних аспеката овог система заштите, а посебно у организационом и нормативном смислу.

Стручњаци који се баве пословима информацијске безбедности имају превасходно информатичко образовање и немају формалну едукацију из области опште безбедности.

Нормативно организовање послова заштите информација у банкама и финансијским институцијама базира се на стварању јединствених основа овакве заштите кроз стварање формалних докумената, који треба да представљају правне механизме за остваривање ове врсте заштите, али који треба и да стандардизују поступке запослених, у смислу остваривања заштите информација, као и да омогуће њену контролну функцију.

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

У будућности се предвиђа раст безбедносних ризика у области информационе безбедности, у банкама и финансијским институцијама, што ће довести до истоврене потребе уже специјализације ангажованих људских ресура по проблемским областима и, са друге стране, до потребе мултидисциплинарног приступа у креирању потребних образовних профила за ове потребе.

8. НАЧИН ИСТРАЖИВАЊА

Комплексност, природа и карактер предмета нашег рада определили су нас за примену већег броја теоријско-емпиријских метода истраживања, и то:

Анализа садржаја ће се углавном примењивати у анализи домаћих и страних извора података као што су стручно-теоријска литература, законски и подзаконски акти Републике Србије и доступна документација Министарства унутрашњих послова и банака и финансијских установа.

Компаративна метода ће се примењивати ради утврђивања сличности и разлика у организиовању и нормативном оквиру при заштити информација у банкама и финансијским установама међу различитим државама.

Статистичка метода ће се примењивати за обраду и класификацију: квантитативних обележја која се односе на предмет истраживања, података прикупљених емпиријским истраживањем, као и других података до којих ћемо доћи кроз процес истраживања.

У истраживању ће се користити, према потреби, и ***посебне научне методе***, као што су: анализа, синтеза, индукција, дедукција, апстракција, и генерализација.

I ПРЕГЛЕД РЕЛЕВАНТНИХ НАУЧНИХ РАДОВА

Поред теоријско концептуалног оквира који је представљен у претходном делу, учинило нам се значајним да детаљније изложимо кључне налазе аутора који су се у својим (углавном докторским радовима), бавили концептима који су окосница и овог рада. Ови радови су интересантни и са аспекта методолошког приступа и резултата до којих су дошли у својим истраживањима и анализама. Њихови резултати су била и нека врста смерница или подстицаја, приликом конципирања истраживачких задатака и избора приступа у представљању сопствених налаза и резултата.

i. Разумевање и мерење културе информационе безбедности у земљама у развоју: случај Саудијске Арабије

У својој докторској дисертацији о разумевању и мерењу културе информационе безбедности у земљама у развоју: случај Саудијске Арабије, аутор има амбицију да премости разлику између фактора који чине (информациону) безбедносну културу и фактора који на њу утичу.[48] Такође, научни циљ је постављен тако да ово истраживање може да представља полазиште за будућа слична истраживања, где ће истраживачи моћи да модел за мерење информационе безбедносне културе примене и у другим амбијентима (у односу на Саудијску Арабију), а посебно да ће на овај начин истраживачи моћи да обављају оваква компаративна истраживања (између развијених и неразвијених земаља).

Аутор уочава да се у току оваквог истраживања његова пажња мора кретати на такав начин да се подједнако уважавају особине националне и организационе културе које могу утицати на практично остваривање информационе безбедности и − техничких питања која су од значаја за овакво истраживање.

Посебну вредност у овом истраживању, полазећи од нашег предмета интересовања, има део у којем аутор прави анализу досадашње научно истраживашке праксе. У том смислу, у овом раду аутор је анализирао тринаест, за његово истраживање референтних радова и том приликом је мерио учесталост појединих проблемских области које су аутори третирали истражујући информациону безбедносну културу. Тако је установио листу проблемских области, где највећу учесталост имају следеће теме:[49]

- подршка менаџмента информационој безбедности;

[48] Alnatheer. M. A.: *Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia,* PhD Thesis, Faculty of Science and Technology, Queensland University of Technology, Brisbane, Queensland, Australia, 2012.
[49] *Ibid,* стр. 45

- политике и спровођење информационе безбедности;
- свест о информационој безбедности;
- тренинг о информационој безбедности;
- процена ризика у информационој безбедности;
- контрола усклађености у информационој безбедности;
- организациона култура;
- правила понашања.

Према ставу истраживача, сигурност информација и њено управљање баве се[50]:

- људима;
- процесима;
- технологијом.

Технологија је сама по себи релативно објективна, а на људе и процесе утиче окружење у којем они делују. На људе и процесе утиче људско понашање, што како аутор даље закључује, може утицати на управљање информацијском сигурношћу. Он наводи да су бројни научни радови који подупиру став да људска димензија чини најслабију везу у информационој безбедности, одакле је стварање безбедносне културе од суштинског значаја и неизбежно, како би организације побољшале ефикасност управљања информацијском сигурношћу.[51]

Према мишљењу аутора, значај овог рада лежи у концептуализацији и истраживању фактора који представљају културу безбедности. Испитивање културе информатичке сигурности је врло сложено, што произилази из служености окружења које ствара такву културу. Такође, велики изазов за ово истраживање било је разумевање фактора који утичу или стварају ову културу, одакле су многи ови фактори у раду испитивани, укључујући разумевање односња између самих фактора и фактора који одражавају културу безбедности.

Одатле се и сам истраживачки проблем може дефинисати као питање одређивања карактеристика које концептуализију модел мерења културе безбедности информација (за организације у Саудијској Арабији). У ту сврху, како би се решио постављени проблем, коришћени су квалитативни интервјуи, који су открили факторе који утичу на безбедносну културу. На основу добијених резултата (фактора) извршено је синтеза како би се развио модел мерења. Затим су кориштени квантитативни инструменти за тестирање и потврђивање самог модела. Да би се решио постављени истраживачки проблем, формирана су три истраживачка питања и то:

- који су то фактори који одређују или одражавају безбедносну културу;
- који су фактори који директно утичу на безбедносну културу;
- како се може развити поуздан модел мерења културе безбедности информација.

[50] *Ibid*, стр. 245.
[51] *Ibid.*

Добијени резултат је био да се култура безбедности може конституисати размишљањем о три главна фактора и то:

1. Безбедносној свести
2. Усклађености културе безбедности са самом сигурношћу
3. Постављањем питања о власништву безбедности

Поред тога, утврђено је да су фактори који потичу на безбедносну културу:

- учешће управа (највишег менаџмента) у информационој безбедности;
- спровођење (неспровођење) политике информационе безбедности;
- безбедносна обука запослених;
- политика (одређивање) етичког понашања.

Добијени налази показују да је безбедносна култура позитивно повезана са безбедносном свешћу и безбедносним власништвом. Фактори који утичу на безбедносну културу позитивно су повезани са укљученошћу највишег менаџмента, спровођење политика и обуком. Поред тога, добијене су позитивне корелације између фактора који утичу на безбедност и фактора који чине или одражавају културу безбедности.

Полазећи од предмета нашег истраживања, потенцирали би став аутора да се област безбедности информација односи на људе, процесе и технологију. Најмања неизвесност, у смислу ефикасности, према нашем мишљењу, долази из сфере технологија. Такође, овом погледу би додали и наше уверење да се систем безбедности не састоји само од технолошког дела, односно онога што чини технологију (са својим средствима, правилима, мањкавостима које се непосредно одражавају на рањивост система и друго), већ се састоји и од других елемената (система) који не припадају информатичкој делатности. Ако ово гледиште сведемо на предмет наведеног рада, онда можемо закључити да људи и процеси које они обављају и организују заиста чине важне делове информационе безбедности, као и да се технологија, како каже аутор предметног рада, потпуно оправдано третира као важан део информационе безбедности, али и да се истовремено, наше је мишљење, информациона безбедност никако не може сводити само на технологију, односно на оно што представља начин на који људи обављају своје процесе.

ii. Управљање информационом безбедности: студија случаја културе информационе безбедности

Савремено управљање информационом безбедности, према мишљењу аутора, поред традиционалног приступа који у првом реду разматра питања технолошких решења у заштити информација, пред себе треба да поставља као императив и укључивање

људи и процеса који они обављају.[52] На тај начин, рађа се потреба за друштвено-техничким приступом у фокусирању на ова питања, а посебно у земљама које се налазе у технолошком развоју (истраживање је спроведено у Саудијској Арабији).

Људски фактори представљају кључно питање које менаџери морају да реше да би се остварило ефикасно управљање сигурношћу информација. У том контексту аутор износи дилему да ли су постојећа научна сазнања, која су развијена углавном у развијеном свету, примењива у земљама у развоју, полазећи од културолошких разлика, а тиме и од евентуалних разлика у култури информационе безбедности. Одатле и потреба да се идентификују људски елементи који утичу на ефикасност целог система, како би се дизајнирале стратегије које могу умањити слабост система. Због тога је, приликом анализе система безбедности информација, потребно сагледати системе информационе безбедности организација у социо-техничком контексту.
Основно питање које аутор поставља је: Којим организационим елементима је потребно управљати да би се осигурало ефикасно управљање сигурношћу информација у Саудијској Арабији.[53]

Како би дао одговор на ово питање он поставља помоћна питања, и то:

- које су тренутне праксе управљања у вези са управљањем информационом сигурношћу и утицајем на културне факторе у Саудијској Арабији;
- у којој мери организациона и национална култура утичу на праксу информационе безбедности;
- у којој мери релевантне вредности националне културе утичу на ефикасност управљања информационом безбедности;
- у којој мери релевантне вредности организационе културе утичу на ефикасност управљања информационом безбедности;
- како организације могу да стекну квалитетну и успешну културу безбедности информација у односу на предложени оквир који задовољава потребе.

Предмет нашег истраживања нас је упутио да посебну пажњу обратимо на модел културе информационе безбедноси који аутор нуди као одговор на постављена питања, не разматрајући их на овом месту у појединости.

Алфаваз у том објашњењу тврди да је поред улоге технологије (пренесено на смисао нашег истраживања – поред IT безбедности) кључну улугу у култури информационе безбедности има улуга менаџмента. Они заједно утичу на вредности које су некада видљиве а некада не. Те вредности, заједно са активностима које здружено пружају технологија и активности менаџмента стварају праксу која може бити различита у погледу статуса знања и активности запослених. У том смислу аутор разликује следеће ситуације које он одређује као посебне модове организације: [54]

[52] Alfawaz, S. M.: *Information security management: A case study of information security culture*, Faculty of Science and Technology, Queensland University of Technology, 2011.
[53] *Ibid*, стр. 241.
[54] *Ibid*, стр. 226. – 233.

МОД 1: Нема знања, нема активности	МОД 3: Има знања, нема активности
МОД 2: Нема знања, има активности	МОД 4: Има знања, има активности

Једини прихватљиви мод за организацију је када постоје знања (развијена технолошка знања и вештине, проактивна сарадња са другим пословним функцијама у организацији, дефинисане политике безбедности и друго) и када се запослени понашају у складу са прокламованим вредностима (видљивим и невидљивим) и добијеним инструкцијама (свест о безбедности).

iii. Друштвено-организациони приступ управљању безбедности информационих система у контексту интернет банкарства

Рад представља социјално и организационо гледиште за проучавање система безбедности информација у области интернет банкарства.[55]

Несумњиво је да интернет пружа огромне могућности да предузећа прошире своју инфраструктуру и побољшају доступност својим клијентима, као и да се смање трансакциони трошкови и побољша ефикасност ових организација.

Са друге стране, интернет представља и канал којимо се остварују претње које ометају посао. Временом, развијени су бројни и ефикасни системи који су пре свега технички оријентисани и који занемарују и игноришу социјалне аспекте ризика и неформалне структуре организација.

Овај рад, заснива се на претпоставци да се безбедност информационих система може посматрати само кроз системско и свеобухватно проучавање различитих аспеката друштвене организације (технички аспект се том приликом не доводи у питање).

У ту сврху Коскокас свој приступ предмету истраживања нуди кроз концепт посматрања пирамидалног модела, користећи претходна истраживања у друштвеним наукама, одакле испитује односе (повезаност) између појмова поверења, културе и комуникације. На основу предложеног модела пирамиде перформанси наглашава се важност и међусобна повезаност различитих друштвено−организационих аспеката и истом приликом се показује вредност сваког аспекта у безбедности информационих система.

---

[55] Koskosas, I. V.: *A Socio-Organizational Approach to Information Systems Security Management in the Context of Internet Banking*, A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing at St. John's Brunel University, London, UK, 2004.

У осврту на дотадашњу праксу (успостављања система безбедноси информација у интернет банкарству) и прегледајући научне радове из ове области, аутор препознаје четири раличите фазе и то: Прве две генерације имају за циљ да открију шта се може учинити у отклањању претњи, па с тога доминирају принципи, чек листе и већина безбедносних стандарда за развој система. Трећа генерација укључује моделирање, а четврта наглашава управо социотехнички дизајн.[56]

Полазећи од предмета истраживања нашег рада, на овом месту нећемо детаљније приказати понуђени Модел пирамиде перформанси, али ћемо навести да аутор сматра да се он састоји од: поверења, културе, комуницирања приликом ризика, постављених циљева, селекције циљева и високе посвећености организације реализацији постављених циљева.[57]

Истраживање (интервјуом) је спроведено тако да су се користиле три студије случаја, у три одељења IT-а, у три различите банке у Грчкој. Банке су одабране тако да су по критеријуму њихових финансијских средстава, заступљене мале банке (Алфа банка), средње банке (Делта банка) и велика банка (Омега банка). Разлог оваквог избора студије случаја је провера да ли предложени Модел пирамиде перформанси је универзалан за све (ове три) структуре IT група. Алфа банка је тада имала у IT-у 60 запослених, Делта банка 150 запослених, а највећа, Омега банка, 410 запослених у IT-у. По структури власништва, такође су заступљена приватна банка (Алфа), полу јавна (Делта) и јавна банка (Омега банка).

Полазећи од наше хипотезе истраживања, и прегледом рада Коскокаса, приметили смо да је истраживање спроведено тако што су се интервјуи спроводили са претежно запосленима у IT-у, а тек местимично се појављују и остале пословне функције *(E-banking manager, Audit manager, Organization manager, Marketing manager, Alternative network manager i Strategic plan manager*)[58]. Наше је мишљење да је овакав избор саговорника, са једне стране позитивно искуство, јер у нашем хипотетичком оквиру управо износимо претпоставку да се информациона безбедност не може сводити само на *IT security,* већ да је реч о ангажовању свих потенцијала организације (као што су, поред наведених у истраживању, *Phisical security, Compliance, HR, Legal*, односно друге послововне функције у банци), док је са друге стране пожељно да се у оваквим истраживањима друге пословне функције (ван IT-а) обухвате у већој мери[59].

Наше је мишљење да је аутор свестан оваквог одређивања снага информационе безбедности у банкама, јер у закључним разматрањима износи тврњу да модел јесте потврђен, али и да ће он у пракси помоћи, као концептуални модел, IT менаџерима и практичарима. Та корист се огледа, према аутору, у побољшању ефикасности процеса постављања циљева и према томе, ефикасном управљању заштите информација у контексту интернет банкарства.

[56] *Ibid*, стр. 4.
[57] *Ibid.,* стр. 41.
[58] *Ibid.,* стр. 72. – 73.
[59] Називи пословних функција су наведени на енглеском језику, будући да је таква пословна пракса, посебно у банкарском сектору, о чему ће више речи бити касније у раду

Даље, аутор у закључним разматрањима наводи да је емпиријски потврђено кроз три студије случаја међусобна повезаност поверења, културе и комуникације и да ти социоорганизациони аспекти имају крајњи ефекат на ниво постављања циљева. Важно је напоменути да је примећено да су ови односи, односно у крајњем ефекат, израженији у организацијама са малом величином стуктуре. Разлог – овакве организације показују „породично оријентисане“ пословне обрасце, јер се вредности и уверења снажно држе и деле међу њеним члановима. Истини за вољу, и велике организације имају овакву димензију, али је у знатно мањој мери. Разлог – овакве организације у великој мери зависе од приручника и процедура (ми би рекли да зависе од формално утврђених правила и некада ригидног приступа донетим процедурама рада), на које се фокусирају строги, професионални критеријуми, а не појединачна иницијатива и интелект.[60]

Коскокас даље закључује, да су концепти поверења, културе и комуникације блиски и међусобно повезани, али и да нису увек међусобно зависно променљиве. То значи да ови аспекти могу постојати унутар организације независни један од другог. На пример, култура у организацији може бити јака, али ниво поверења низак, иако јесте утврђено да поверење олакшава успостављање снажне културе унутар организација и ефикасност комуникације коју треба постићи.[61]

Поверење, дефинасано као спремност једне стране (појединца) у оквиру IT група да сарађује са другом страном у циљу ефикасног рада, игра важну улогу на нивоу постављања циљева. На пример, када су запослени задовољни поступањем топ менаџмента, они имају осећај да су напори и радни резултати оправдани (или финансијски награђени), па су тако мотивисани да учествују даље у раду групе.[62]

iv. Безбедност електронског банкарства и организационе промене

Предмет истраживања овог рада је акционо истраживање безбедности корисника електронског банкарства у једној великој евроспкој банци.[63]

Акциона истраживања представљају флексибилни процес у коме се смењују акција (промена, побољшање) и истраживање (разумевање, знање). Ограничена су на област у којој се спроводи акција и на узорак испитаника на који се акција спроводи, одакле нису погодна за уопштавања (односне се на конкретан проблем). Она теку паралелно са проблемом који се истражује, тако што се прате промене до којих долази. Из овог разлога ова истраживања често не теку по плану, него се мењају током акције, а поједине фазе се понављају.[64]

---

[60] *Ibid.*, стр. 191.
[61] *Ibid.*, str. 192.
[62] *Ibid.*
[63] Birkeland, S.: *E-Banking security and organisational changes*, PhD thesis, University of Liverpool, 2015.
[64] Наведено према: Максимовић, Ј.: *Матрица планирања акционих истраживања*, прегледни чланак, Филозофски факултет, Ниш, 2012. година. Доступно на адреси: https://scindeks-clanci.ceon.rs/data/pdf/0353-7129/2012/0353-71291202231M.pdf

Околности које чине амбијент израде овог рада су чињенице да је (изражени) развој електронског банкарства на неки начин створио јаз између перцепције запослених у банци и корисника услуга, у вези са безбедношћу. Прелазак на дигитално пословање, изазвао је банке да у само неколико година створе нова (безбедна) решења за своје купце. Са једне стране постоји захтев корисника за општом и лаком доступношћу дигиталних сервиса (са чиме се банке слажу у смислу постизања боље продаје својих производа), а са друге постоји забринутост запослених у банкама да ти сервиси неће бити довољно безбедни или бар не безбедни на нивоу услуга традиционалног банкарства. Клијенти банке нису склони да одмах размишљају о могућностима нових приступа нарушавања њихове безбедности, као што је социјални инжењеринг.

Биркланд наводи да савремена дигитална банка не треба да делује као традиционална банка, већ више као IT компанија[65]. Ова тврдња отвара пут новим идејама и решењима, спајањем банкарског посла и рачунарске индустрије. Изазов је професионална удаљеност ових група, одакле будуће реорганизације требају да теже њиховој сарадњи повећавајући интерно комуницирање и контакт са клијентима. Ове промене не смеју никада да забораве на главни ресурс и претњу безбедности – на људска бића.

Аутор износи став да безбедност није само физичка заштита зграда, или заштита страница за пријаву на интернету, већ је то начин размишљања, који због насталих промена захтева континуитет у планирању и анализи. Банкарска индустрија се због тога променила и она подржава растуће тржиште коришћења мобилних уређаја за банкарство. Уместо ранијег једног канала пословања, сада истовремено постоји више канала.

Биркланд се у раду критички осврће на дотадашњи приступ теорије, где су научници чак почетком овог миленијума износили ставове из којих следи да је безбедност технички фактор[66]. Аутор истиче да је ова разлика кључна не само за његов рад, већ да је реч о неминовности у промени концепта безбедности, који доноси модерно банкарство. Захваљујући интернет банкарству, безбедност постаје друштвени проблем, у којем се јављају и нове методе угрожавања (као што је *phishing*).
С тим у вези, у раду се одређују главна питања којима ће се савремене банке бавити, када је у питању сигурност корисника, и то[67]:

- потрага за дефиницијом савремене банке;
- које су одговорности менаџмента (лидера);
- које су одговорности запослених;
- како дефинисати безбедност;
- која је стратегија безбедности корисника;
- који су предлози за будућа решења.

Потрага за дефиницијом савремене банке подразумева да ће бити потребно препознати шта је то модерна банка. Посао се трансформише из физичког контакта са

[65] Birkeland, S., *op.cit*., стр. 8.
[66] *Ibid*., стр. 39.
[67] *Ibid*., стр. 94.

купцима као основног елемента у профил где се банкомати (*ATM*) и *PC* рачунари замењују преносним рачунаром, таблетом и мобилним телефоном. За само неколико година од писања овог текста, можемо да констатујемо да је то време већ дошло, а да се плаћања већ увелико одвијају преко мобилних платформи, где на пример, у Кини, просјаци примају добровољне прилоге претходним очитавањем QR кода са њиховог телефона[68]. Банка постаје сродна IT корпорацији, где њени купци представљају различите групе – од предузетничких радњи, малих и средњих предузећа, великих организација, па до глобалних корпорација и владе. Све ове групе клијената имају различита мишљења о томе шта је сигурна банка и сви имају различите рутине и поступке за руковање својим банкарским пословањем. Тренсфер новца се може обавити било где у (дигиталаном) свету, одакле долази и претња са потенцијалним преварама, прањем новца и финансирањем тероризма.

Полазећи од предмета нашег истраживања, на овом месту би се осврнули на снаге које морају бити укључене у систем заштите информација у банкама. Да ли се традиционални IT сектор онда може самостално бавити овим изазовима? Да ли се онда Информациона безбедност може сводити само на технички аспект? Наше је мишљење исказано у хипотетичком оквиру нашег истраживања, где наводимо да је неопходно овим пословима приступити интердисциплинарно, са ангажовањем свих расположивих потенцијала. У конкретном коментару на тврдњу Бирканда, где смо застали у тексту, потребно је ангажовати и пословне функције спречавање прања новца, спречавање превара, односно другу пословну функцију која поседује специфична знања за неки део технологије посла који се обавља у банци. Сви ови потенцијали требају бити ангажовани кроз активности пословне фунцкије Безбедности, где се у зависности од претњи, под координацијом сектора безбедноси, формирају привремена и стална радна тела. Другим речима, поседовање специфичних знања у некој области не може бити гарант да ће вође оваквих тимова имати могућност да сагледају довољно широку слику која обухвата све аспекте претње. Такав фокус, наше је мишљење, могуће је имати само из перспективе пословне функције безбедности, која у идеалној ситуацији предтавља једино место у банци где се сусрећу релевантне информације о претњама и инцидентима, и једино место које има свест о потенцијалима које је потребно ангажовати.

Бирканд као поређење промене улоге које сада имају модерне банке користи пример који нам долази из аутомобилске индустрије Тесла. Он каже да је Тесла много више IT компанија, него што припада традиционалној ауто индустрији, и ако је главни производ аутомобил. Тесла приоритетно има потребу за сигурношћу, ажурирањем софтвера аутомобила на мрежи, и иначе све се обавља путем онлајн решења.[69] На исти начин банке управљају новцем људи или компанија, којом приликом је већина контаката са купцима на мрежи. На исти начин успех Тесле показује да нови правци,

---

[68] Независне новине, *Кинески просјаци новац прикупљају уз помоћ смартфона*, доступно на: https://www.021.rs/story/Info/Nauka-i-tehnologija/177828/Kineski-prosjaci-novac-prikupljaju-uz-pomoc-smartfona.html

[69] Birkeland, S., *op.cit.*, стр. 94.

раскид са традицијом и одважност у том смислу, могу бити важни елементи пословног успеха, закључује аутор.

Које су одговорности менаџмента (лидера) је питање које извире из такве промене организације где се лидери не налазе, у физичком смислу на истом месту где и чланови њиховог тима (подсећања ради, Бирклaнд у овом акционом истраживању има у виду банку која ради у више земаља). Бројна су отворена питања која је потребно даље изучавати у овој области, али овде аутор претпоставља да ће културолошке разлике конкретне средине имати значајан утицај на одређивање одговорности менаџмента.

Које су одговорности запослених је проблемска област која се јавља при преласку фокуса са лидета на запослене, где свакако постоји питање поверења и одговорности. Задатак запослених је да стварају и одржавају контакт са купцима, дефинишу потребе купаца и пружају менаџменту (лидерима) одговарајуће информације за развој добрих пословних стратегија. Одговорност ту није спортна, она мора да постоји, али важније од тога је развијање култура, свести запослених и иновативно понашање (запослених) изнутра, што нас у коначном води ка самолидерству запослених.

Како дефинисати безбедност, у овом раду је питање које се односи на безбедност купаца, односно на питање како они доживљавају безбедност. Не треба да изненађује да у овом истраживању клијенти безбедност на мрежи доживљавају као најважније питање, што се у крајњем своди на њихово поверење према банци. Нове претње се догађају свакодневно. Превара, хаковање и сајбер криминал се повећава, али купци (у овом акционом истраживању) остају и даље сигурни и задовољни. Из ових разлога, наводи аутор, кампање за подизање свести могу постати важније од стварања опипљивог решења, јер људске грешке узрокују већину инцидената и кршења.[70]

Задатак је дакле створити осећај код купаца да је сигурност добра. Хардверска и софтверска решења је тешко објаснити купцима, али је и то неопхоно, али нетехничким језиком – како би се створило поверење. Нематеријална безбедност ће проактивно радити на информисању купаца о социјалном инжењерингу, тако да смањи вероватноћу да ће они кликнути на злонамеран линк на веб страницама или у *e-mail*-у, односно да ће избећи веб странице које могу садржати вирусе или тројанце. Треба помоћи купцима да разумеју важност коришћења јаких лозинки, као и да схвате да се личне информације не дају било коме (и/или када за тим нема потребе). Социјални инжењеринг постаје све већи проблем, будући да хакери користе метод лова са минималном интеракцијом – супротно начину када успостављају ближе везе током дужих периода. Банке морају имати довољно техничких решења на располагању за отривање злонамерног понашања када се хакерима омогућава довољно информација од купаца да изврше напад. Тако се ствара поверење, јер се клијенти ослањају на банку да има доступне филтере за преваре. Кампање за подизање свести о преварама код купаца требало би да дају најбољи резултат у спречавању ових дела. У том смислу исправно је да безбедносна стратегија мора препознати безбедност као производ који се продаје, а не да представља трошак.

[70] *Ibid.*, стр. 105. – 106.

Која је стратегија безбедности корисника је питање које се односи на пословна и техничка решења, где треба тежити двосмерном комуникацијском процесу. Најбољи пример је питање аутентификације корисника приликом пријаве на систем, где огроман број решења указује да је за очекивати да ће се на овом пољу догађати инциденти (систем трага за ефикасним решењем). Парадоксално је, али и истинито, да се тежи поједностављењу аутентификације, а Биркланд оставља отворено питање да ли је то у корист банке или у корист клијента.[71]

Који су предлози за будућа решења, аутор наводи читав низ предложених активности[72], а полазећи од нашег предмета истраживања ми ћемо на овом месту, без детаљнијег осврта навесети да је реч о декларативном прегледу мера које треба да донесу бољу унутрашњу комуникацију, више иновација, инкременталне промене (насупрот револуционарним), ефикаснију организацију рада, и друго.

v. Анализа упоређивања препорука најбоље праксе и законских услова приликом подизања свести кућних корисника онлајн банкарства

Овај магистарски рад за предмет истраживања има искуства јужноафричких кућних корисника интернета за обављање различитих послова који укључују, али нису ограничене, на куповину преко мреже, онлајн игара, али и банкарско пословање.[73]

Полазећи од предмета истраживања нашег рада, привукао нам је пажњу са аспекта проблема подизања свести корисника о безбедности приликом онлајн банкарства (енгл: *security awaraness*), где банке, видели смо из досадашњег прегледа научних радова, посвећују посебну пажњу у склопу изградње сопственог система заштите информација.

Вишеструке су претње којима су корисници изложени, а најчешће се говори о *Phishing*-у[74] и Социјалном инжињерингу. Ми ћемо у нашем раду у каснијим разматрањима посебну пажњу обратити овим претњама, будући да искуствено знамо да је реч о честим облицима угрожавања.

Када су у питању јужноафричке банке, ауторка наводи да постоје и одређене законске обавезе банака у смислу борбе против ових напада, које се спроводе преко

[71] *Ibid.*, стр. 107.
[72] *Ibid.*, стр. 108.
[73] Lee Botha, C.: *A Gap Analysis to Compare Best Practice Recommendations and Legal Requirements when raising Information Security Awareness amongst Home Users of Online Banking,* Submitted in accordance with the requirements for the degree of Master of Science in the subject Information Systems, University of South Africa, 2011.
[74] Пецање (енгл: *Phishing*) или мрежна крађа идентитета представља покушај крађе података корисника интернета путем фалсификоване веб странице. Обично се таква лажна страница нуди путем посебно припремљене е-поруке или ћаскања. Пошиљалац тако наводи жртву да преко телефона или лажне странице чија је хипервеза дата у поруци, пошиљаоцу открије поверљиве информације. Те информације он користи у разне сврхе, али најчешће за крађу новца с банковног рачуна или за провалу у е-пошту жртве.

иницијативе за подизање свести корисника. У случају неусклађености или непоштовања ових обавеза банке су изложене кажњавању, поред могућих штета бренда и губитка клијената банке (касније у нашем раду видећемо да је реч о *Репутационом ризику* где постоји и норматива од стране централних банака). Поред ових обавеза, Либота у свом раду наводи и примере најбоље праксе у погледу заштите информација, да би на крају извршила анализу празнина које се јављају када се упореде најбоља пракса и законске обавезе банака, одакле закључује да ова два аспекта нису до краја усклађена, те да је у том смислу потребно организовати адекватне контроле.

Наше је мишљење да овај рад може користити будућим истраживањима, пре свега као идеја за методолошки оквир акционих истраживања које банке могу спроводити у циљу унапређења свести о безбедности својих корисника (купаца) приликом онлајн банкарства[75], као и ефикасног прегледа стања где се нека банка налази у погледу предметног развоја.[76]

vi. Управљање пословима *IT* безбедности – упоредна студија у Пакистану и Краљевини Шведској

Полазећи од широке примене интернета у пословању компанија, аутори одређују предмет истраживања као критички преглед на то како различите врсте пословања управљају својом *IT* безбедношћу у Пакистану и у Шведској, са нагласком на административну контролу додељених привилегија. [77]

Полазећи од предмета нашег истраживања, а посебно од нашег хипотетичког оквира, запажамо да се овде заштита информација фокусира на технички аспект заштите (а чак и том смислу заштиту третира само једним, малим делом), док се сви остали безбедносни подсистеми занемарују.

Како је, према мишљењу аутора, *IT* безбедност начелно добро организована захваљујући дефинисаним процедурама (они кажу да постоји „списак корака“), аутори су се сконцентрисали на три главне функције, и то:

- политка *IT* безбедности;
- план *IT* безбедности;
- анализа безбедности *IT* ризика.

[75] Carla-Lee Botha, *op.cit*., стр. 7.
[76] *Ibid*., стр. 150.
[77] Khalid, F., Qureshi, M. A.: *How companies manage IT security A comparative study of Pakistan and Sweden,* master thesis in informatics, Jönköping International Business School, Jönköping University, Sweden, 2013.

Даље, аутори су сами приметили да немају репрезентативност узорка истраживања, будући да су истраживањем обухватили само једну шведску (Универзитет у Јанћепингу) и три пакистанске компаније.

Наше је мишљење, да уско гледање на области заштите информација у овом раду произилази из дефинице *IT* безбедности коју су аутори понудили у уводном излагању, а према којој она представља свеобухватни аспект у погледу информационих система, а укључује процедуре, сигурносне политике и безбедносне мреже, базе података, дата центре, који опет укључују сервере и радне станице.[78]

Према нашем мишљењу, претходно наведени ставови нису ненамерна грешка аутора, већ је реч о суштинском неразумевању заштите информација, онако како је ми разумемо и како је третира научна јавност, а што смо видели у досадашњем прегледу научних радова за потребе наше рада.

Политка *IT* безбедности, како је наводе Калид и Али Кureши, представља основни документ управљања сигурношћу информација. На њој (политици) су засноване процедуре и под политике. Политика мора бити кратка и концизна, како би била прихватљива извршном руководству и менаџменту, како би ови били у прилици да је подрже.

План *IT* безбедности, према ауторима овог рада, има задатак да смањи *IT* ризик путем контроле. Оне се могу спровести извођењем вежбе, којом приликом закључивања треба имати у виду примере најбоље праксе.

Анализа безбедности *IT* ризика има задатак да припреми организацију на могућност губитка инфраструктуре информационих система, одакле је потребно ове ризике идентификовати и анализирати њихове последице.

У закључним разматрањима аутори не наводе систематизоване закључке из свог истраживања, већ понављају *ah hoc* оцене које су дали у уводним разматрањима ове (педесетак страница обимне) студије.[79]

Наша је првобитна идеја била да услед броја и природе примедби које имамо на структуру рада, спроведену методологију истраживања и начин посматрања предмета истраживања, овај рад одбацимо у прегледу научних радова из наше предметне области, али смо на крају мишљења да је потребно приказати и овакав приступ изучавању у заштити информација и информационих система – посебно јер искуствено опажамо да се овакво, вулгарно и ненаучно гледиште често може пронаћи у пракси, посебно када је у питању пракса остваривања *IT* безбедности (фаворизовање техничких знања и вештина на рачун свих осталих области које чине заштиту информација, чиме се у крајњем урушава сам систем безбедности организације).

[78] *Ibid.*, стр. 4.
[79] *Ibid.*, str. 42 − 46.

vii. Кибер ратовање – нови облик савремених друштвених конфликата

Путник у својој докторској дисертацији показује како се кибер ратовање помера из војне сфере на индивидуалну, друштвену и комерцијалну раван. Он предмет свог истраживања дефинише као идентификацију и класификацију савремених облика сукобљавања у кибер простору. [80]

У операционом смислу, аутор феномен кибер ратовања посматра кроз друштвени контекст у коме он настаје, па тако разматра генезу и теоријско одређење појмова: информациони системи, кибер простор, Интернет, информационе инфраструктуре и информационо друштво. Такође, приказана је и генеза концепта кибер ратовања, да би потом конфликтолошком анализом посматрао елементе структуре конфликта. На овај начин дошло се до сазнања о актерима кибер ратовања, објектима тог ратовања и методама и средствима који се користе приликом конфронтација у кибер простору.

Полазећи од предмета нашег истраживања, пажњу нам је привукло разматрање Путника о техничко-технолошким узроцима несигурности кибер простора. Он каже да је проблем рањивости у имеративној комерцијалној употреби хардвера и софвера. Реч је о томе да је пажња произвођача ових компоненти усмерена на брзину лансирања нових производа, на рачун безбедности и поузданости. То даље ствара слабости које постају основа неправилног функционисања рачунарских система. Ове рањивости представљају слабости које се могу искористити за извршавање неауторизованих и нелегитимних акција у мрежи или систему. Искоришћавање те прилике од стране злонамерних извршилаца ствара безбедносни инцидент, а број тих инцидената са временом расте великом брзином.

Несигурност кибер простора има двојаку основу, и то су:

- технички разлози;
- грешке и пропусти организације и индивидуалних корисника приликом коришћења („људски фактор“).

Ова, друга група, посебно привлачи нашу пажњу, обзиром да како Путник наводи, она се уопштено може повезати са недостатком пажње, а неретко и недостатком образовања корисника о безбедности сопствених система. Ми смо у досадашњем прегледу научне литературе, као и искуственим опажањем, ово становиште сусретали код проблема подизања нивоа свести код корисника (енгл: *security awareness*), који са аспекта банкарског пословања могу бити и клијенти, али и сами запослени банке.

Уосталом, Путник наводи да је *недостатак безбедносне културе* уочљив и на индивидуалном и на нивоу предузећа и организација, што је у сагласности и са нашим хипотетичким оквиром. Аутор наводи да вртоглаву експанзију Интернета не прати и

[80] Путник, Н.: *Кибер ратовање – нови облик савремених друштвених конфликата*, докторски рад, Факултет безбедности, Универзитет у Београду, Београд, Република Србија, 2012. година, стр. 15.

одговарајућа специјализација стручњака на пољу информационе безбедности, па тако цитира Е. Спафорда (E. Spafford), директора Центра за едукацију и истраживање у области информационог осигурања и безбедности универзитета Пардју (енгл: *Purdue University, Public university in West Lafayette, Indiana, USA*): „Безбедност није могуће лако додати накнадно, што знатно отежава задатак професионалцима безбедносног сектора. Софтвер и хардвер који се данас користе пројектовани су неправилним методима, а такође се накнадно лоше тестирају, од стране особа које знају мало или готово ништа о безбедности, што је резултовало непоузданим резултатима. Затим се додају постојећој инфраструктури, која је већ пуна слабости и којом управља, и користи је, особље недовољно упознато са ризицима. Нико не би требало да се изненади повећањем броја напада и вируса у годинама које следе.“[81]

Путник, даје преглед субјеката кибер ратовања:

Табела бр. 1: *Класификација субјеката претњи у кибер простору*[82]

Субјекти претњи	Мотивација	Технике и инструменти
Хакери Крекери	Изазов Его Бунтовништво	Социјални инжењеринг Неауторизовани приступ Малициозни програми
Хактивисти	Пропаганда Праћење политичких циљева	Опструкција услуга „Изобличавање“ сајта (енгл. web defacement)[83]
Инсајдери	Радозналост Его Обавештајна активност Материјална корист Освета	Уношење погрешних или лажних података Прислушкивање („пресретање“) Малициозни програми Саботажа Неауторизовани приступ Социјални инжењеринг
Криминалне групе	Уништавање информација Илегална дистрибуција информације	Напади уз коришћење обмане Крађа идентитета

[81] *Ibid.*, str. 83. – 87.
[82] *Ibid.*, str. 203.
[83] Енгл: *defacement* (као и његов синоним енгл: *defacing*) могао би се дословно превести са „наруживање“, „замрљавање“. У пољу информационе безбедности овај израз се односи на недозвољено мењање почетне стране неког web сајта (његовог „лица“, home page-а) или преправљање и замењивање једне унутрашње стране или више њих. Овим недозвољеним активностима „наруживања“ сајтова баве се крекери. Мотиви вандализма могу бити различити, од идеолошких до чисте жеље за доказивањем. За добијање приступа сајту-жртви крекери најчешће искоришћавају слабости софтвера који управља сајтом или оперативних система, а ређе се служе техникама социјалног инжењеринга

	Материјална корист	Упад у системе Малициозни програми
Теротисти	Уцена Деструкција Пропаганда Освета Медијска промоција	Информационе операције Опструкција услуга Упад у системе Малициозни програми
Привредни субјекти	Економска шпијунажа Индустријска шпијунажа	Крађа информација Социјални инжењеринг Неауторизовани приступ
Националне армије Обавештајне службе	Стратешка предност	Информационе операције

Нама је приказ изнет у табели, полазећи од предмета нашег истраживања, и са аспекта одређивања области где треба тражити упориште за изгрању система безбедности информација, односно одакле се назире простор који је потребно попунити да би та заштита била адекватна, као и где се може остварити увид колико је погрешан приступ да se заштита информација може остварити само техничким знањима и без знања о безбедности, врло користан и инспиративан за даља разматрања.

Аутор приликом разматрања социо-економског аспекта кибер ратовања примећује да често вокабулар војне терминологије и речник у савременом пословању имају сличности. У оквиру наука о менаџменту често можемо препознати овакве аналогије, као што су термни: стратегија, одбрана, напад, ратови ценама, пословна шпијунажа, предност првог удара и сл.

Појава и успон транснационалних корпорација, као све значајнијих субјеката међународних економских односа, неретко важнијих и од самих држава, јесте једно од најважнијих обележја економске глобализације. Своју глобалну моћ транснационалне компаније остварују путем контроле три најзначајнија тржишта: тржишта роба и услуга, *финансијског тржишта и тржишта информација*. У свим земљама где делују транснационалне компаније, преко ових тржишта се остварује ефективна контрола производње, робних токова, цена, штедње и инвестиција, али и неекономских процеса (политички, културни, идеолошки итд).[84]

Такође, на више места до сада смо истакли, а са тим се слаже и Путник, да је људски фактор једна од најслабијих (ако не и најслабија) карика у систаму заштите лице имовине и пословања.

[84] *Ibid.,* str. 271. - 272.

У раду је приказан преглед перцепције самих запослених, према истраживању о томе са које стране долази претња за безбедност информационг система, према којем је структура претњи таква да око 80% претњи долази од стране хакера и *од стране самих запослених*[85].

Мотивисаност инсајдера за нарушавање безбедности, како наводи аутор, може бити различита и да потиче од:

- другачијег система вредности у односу на организацију која их запошљава,
- радозналости, освете, уцене, изнуде, мотива нелегалне зарада и др.

Аутор новоди истраживање које је обављено за потребе *McAfee*-а, а које је спроведено у Европи 2005. године, о које је показало је да 21% запослених дозвољава пријатељима и члановима породице да, код куће, користе службени рачунар. Најчешће се службени рачунар употребљава за „сурфовање" интернетом, што не само да повећава ризик од инфекције рачунара малициозним програмима (а у перспективи и рачунарске мреже компаније), већ и излаже поверљиве пословне документе неауторизованим лицима; 10% испитаника је признало да са интернета „скида" садржаје за приватне потребе, тј. практикује ризично понашање, с обзиром на то да излаже информационо-комуникациони систем компаније ризику, а послодавца законским санкцијама; 5% испитаника је признало да је направило приступ заштићеним, поверљивим зонама пословног система фирме (мањи број је признао и крађу информација). На основу резултата истраживања дефинисане су четири категорије неодговорних запослених:

- *security softie[s]* („нежна срца") – у ову категорију спада већина запослених. Њих одликује ограничено познавање безбедносне културе; најчешће се ризично понашање ове групе своди на омогућавање приступа рачунарским ресурсима предузећа трећим лицима;
- *gadget geek[s]* („фанатици техничких направа") – у ову категорију сврстани су они запослени који службене рачунаре користе за повезивање са разноразним хардверским уређајима, неауторизованим од стране администратора мреже или лица одговорног за унутрашњу безбедност организације;
- *squatter[s]* („непоштоваоци закона") јесу они који користе ИКТ ресурсе компаније на недозвољен начин (за складиштење и дистрибуцију недозвољених садржаја, играње видео-игара и сличне активности);
- *саботери* представљају, статистички гледано, мали број запослених. У ову категорију сврстани су они који покушавају да приступе заштићеним информацијама или ресурсима ИКТ или, пак, који убацују малициозне програме у рачунарски систем компаније. Најмање су бројни, готово статистички безначајни, али предствљају можда и највећу опасност за заштиту информација организације.

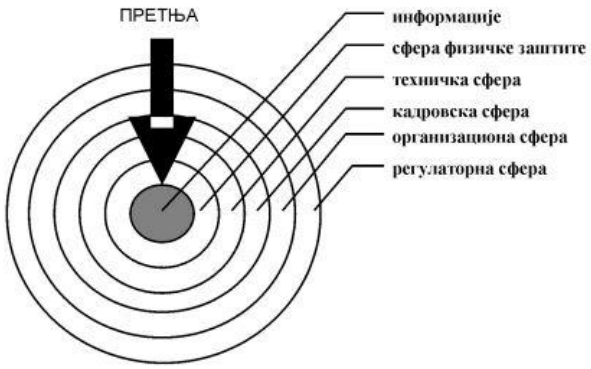
[85] 2003 CSI/FBI Computer Crime and Security Survey, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

Путник у коментару на опасности које доносе сами запослени, који ненамерно наносе штету систему, показује колико је заправо важан људски фактор у остваривању система заштите информација. Једна од могућих стратегија за ублажавање овог ризика је стално информисање запослених о ризицима, организационој политици и безбедносним процедурама. Такође, корисна тежња би била и запошљавање поузданог и поверљивог особља, одакле опет, са становишта нашег предмета истраживања, видимо на примеру колико је важна сарадња више пословних функција у организацији (у овом примеру *HR*-а и безбедносне пословне функције) у остваривању заштите информација. [86]

Полазећи од предмета нашег истраживања, ми смо овом приликом апострофирали улогу самих запослених („инсајдера“) како је то у раду дао Путник, због доказивања значаја људског фактора у остваривању система заштите информација, али сматрамо да је овај рад користан за друга будућа истраживања, тамо где постоји интересовање за друге субјекте претњи како је то аутор приказао у раду (хакери, хактивисти, терористи, криминалне групе, привредни субјекти и друго).

Од посебне је користи за наше истраживање преглед мера и стратегија заштите информационих система, како је то дао Путник. Он наводи да се на основу досадашње добре праксе треба примењивати *Модел вишеслојне заштите*. Модел обухвата неколико аспеката, и одговара претпоставкама када смо разматрали хипотетички овкир нашег истраживања[87].

Схема број 2: ***Модел вишеслојне заштите информација***



Да би претња била реализована, треба да прође више прстенова заштите, и то:

- физичку заштиту;
- техничку заштиту;
- кадровску заштиту;
- организациону заштиту;

[86] *Ibid*., str. 272. – 290.
[87] *Ibid*., str. 362.

– регулаторну заштиту.

Физичко обезбеђење, како наводи Путник, има задатак да онемогући физички приступ информацији, односно информатичким ресурсима. Наше је мишљење, да је потребно скренути пажњу на одређена одступања која се јављају у тумачењу појма физичке заштите, о чему ће касније у нашем раду бити више речи. Суштина је да искуствено опажамо да се под физичком заштитом често подразумева и оно што се код домаћих аутора често назива техничком заштитом, па су у том смислу потребна извесна усаглашавања.[88]

Техничка заштита, представља мере техничког обезбеђења (електронско обезбеђење, идентификаиција, верификаиција и ауторизација приступа, системи за детекцију и спречавање напада и друго). Обухвата и спречавања приступа (физичког и путем мреже) штићеном систему, а у употреби су и различити технички уређаји и средства, као и разноврсни информатички алати.[89]

Организиациона заштита подразумева организациону структуру, дефинисање радног процеса, развој софтверских система, праћење смерница и стандарда, планирање и друго. Подразумева и праћење међународних и националних безбедносних стандарда у овој области. Према намени, они могу бити: стандарди за безбедност производа, стандарди за безбедност процеса и стандарди безбедности система.[90]

Кадровска заштита подразумева планирање и избор кадрова, руковођење, стручно усавршавање, безбедносно образовање (ми смо склони да ову област појмовно одредимо као развој безбедносне свести запослених, енгл: *security awareness*) и друго.

Регулаторна заштита, односно како Путник оригинално назива *Нормативна заштита* подразумева законе, упутства, планове и другу регулативу која обевезује и прописује извршење неке радње и начин извршења те радње. Аутор у свом раду даје упоредну анализу законодавства у Сједињеним Америчким Државама, Великој Британији, Француској, Немачкој, Италији, Јапану, Русији и Кини. [91]

Из модела вишеслојне заштите видимо да наш предмет истраживања (заштита информација у банкама и финансијским институцијама, првенствено полазећи од организационог и нормативног аспекта уређења и обављања ових послова), како смо у хипотетичком оквиру и изнели претпоставку, представља само неке од аспеката заштите информација, али је већ јасно да се та заштита не може свести само на

[88] Физичка сигурност описује мере безбедности које су осмишљене да забране неовлашћени приступ објектима, опреми и ресурсима и да заштите особље и имовину од штете или повреде (попут шпијунаже, крађе или терористичких напада).] Физичка сигурност укључује употребу више слојева међузависних система који могу укључивати *CCTV* надзор, заштитне баријере, браве, контролу приступа, детекцију упада периметара, системе одвраћања, заштиту од пожара и друге системе намењене заштити људи и имовине.
[89] Путник, Н., *op.cit,* стр. 363. – 369.
[90] *Ibid.,* str. 369. – 373.
[91] *Ibid.,* str. 378. – 392.

специфична техничка знања, услед чега се у пракси догађа да појмови IT безбедности и заштите информација представљају синониме – што је погрешан приступ.

viii. Коцепт безбедносне културе и претпоставке његовог развоја

Прегледом научне литературе из области заштите информација банака и других финансијских институција приметили смо да су атрактивни концепти компаративних истраживања у овој области, посебно када су у питању географске области на различитим деловима света, односно географске области у којима је претоставка истраживача да постоје значајне разлике у степену економске развијености друштва, као и где су различити културолошки амбијенти.

Такође, често се у литератури разматра проблематика која се односи на подизање свести о безбедности (енгл: *security awareness*), одакле проблем одређивања безбедносне културе добија на свом значају и актуелности, будући да је наше мишљење да се подизањем свести мења и ниво безбедносне културе.

Ауторка је у свом раду извршила анализу теоријских поставки појмова културе и безбедносне културе.[92] Она је кроз призму културе, националне културе, националног идентитета, концепта безбедности и националне безбедности одсликала својства безбедносне културе као специфичне безбедносне инфраструктуре.

Полазећи од предмета истраживања нашег рада, посебну вредност смо пронашли у разматрањима о појму безбедности, будући да је реч о појму који се у теорији различито дефинише. Станаревић наводи да су бројне дефиниције и тумачења безбедности, те да је тешко определити се која је у том смислу најпрецизнија. Разлог за овакве околности су различити приступи и критеријуми којима су се аутори водили да би објаснили шта безбедност значи. Бројни концепти у дефинисању безбедности резултирали су да су данас у употреби различити (наше је мишљење различити и по својој суштини) изрази: финансијска безбедност, *IT* безбедност, безбедност хране, људска безбедност, друштвена безбедност, здравствена безбедност, енергетска безбедност, правна безбедност и безбедност дома, комерцијална безбедност, као и већ традиционални термин „национална безбедност“.

У нашем истраживању смо, одређујући предмет истраживања и хипотетички оквир, и сами увидели да постоје различити приступи одређивању појма безбедности, па смо тако нагласили да се неоправдано информатичка безбедност (енгл: *IT security)* некада поистовећује са целокупном области заштите информација (енгл: *Information Security* – IS). Искуствено, опазили смо у пракси да се (због свог оправданог значаја за

[92] Станаревић, С.: *Концепт безбедносне културе и претпоставке њеиговог развоја,* докторски рад, Факултет безбедности, Универзитет у Београду, Београд, Србија, 2012. година

функционисње система заштите информација, као и уско специјалистичких знања) некада и цела област безбедности поистовећује са *IT* заштитом.

Станаревић скреће пажњу да треба узети у обзир и чињеницу да безбедност и небезбедност могу бити и резултати процеса (де)*секуритизације*, будући да она представља укључивање многих друштвених питања у расправу о безбедности.[93]

У раду је изнето да се појам безбедности разматра у оквиру бројних научних дисциплина, а ауторка се одлучила да посебно продискутује социолошки, правни, политиколошки и културулошки погледа на безбедност.

Контекст *организационе културе*, који је нама значајан због мотивисаности организације да примењује договорена правила (дакле и правила безбедности), као и да усваја нова знања (програми за развој свести о безбедности) у раду је представљен кроз одређење Едгара Шајна (*Edgar Schein*) најпознатијиg теоретичара који се бавио организационом културом. Он је дефинисао појам организационе културе као образац заједничких основних претпоставки на основу којих је група научила како да решава проблеме спољне адаптације и унутрашње интеграције, а формулисане су довољно добро да се могу сматрати вредним и као такве преносити новим члановима организације, као исправан начин перцепције, размишљања и осећања за исте проблеме.[94]

Такође, ауторка наводи да се организациона култура у литератури назива и *корпоративна култура,* те да се она манифестује у следећем:

- начину на који организација обавља свој посао, третира своје запослене, клијенте, као и ширу заједницу;
- мери у којој су аутономија и слобода дозвољене у доношењу одлука, развијању нових идеја и личном изражавању;
- начину на који моћ и проток информација пролазе кроз хијерархију;
- снази запослених и обавезама према колективним циљевима.

Организациона (корпоративна) култура усмерава, односно чак и одређује свест и понашање људи. Тако људи у једној организацији могу на сличан начин да интерпретирају и разумеју појаве које их окружују. Понашање људи произилази управо из њиховог тумачења света, одакле култура усмерава и одређује и свакодневно понашање и активности људи.[95]

---

[93] Теорију секуритизације је развио Оле Вивер, а она је касније обрађена унутар копенхашке школе студија безбедности. Ова теорија је направила радилан раскид са традиционалним студијама безбедности, које почивају на материјалистичкој претпоставци да безбедносне претње постоје изван дискурса, као и на чињеници да је њихов задатак да претње открију пре него што се оне материјализују. Централно питање традиционалних студија је то како да постанемо безбеднији. Теорија секуритизаицје поставља питање о томе како неко питање постаје и безбедносно питање. Извор: *Опасне везе: теорија секуритизације и шмитовско наслеђе*, Филип Ејдус, Безбедност западног Балкана, часопис београдске школе за студије безбедности, број 13., Београд, 2009. године, стр: 9. – 15. Доступно на: file:///C:/Users/windows%207/Downloads/Opasne_veze_teorija_sekuritizacije_i_Smi.pdf

[94] С. Станаревић, *op.cit*., стр. 243. – 244.

[95] *Ibid*., стр. 244.

Карактеристике корпоративне културе су и да она има сличности, у оквиру различитих организација, али и да истовремено има међусобне различитости. Организациона култура се не мења тако лако.

Како ће се обликовати и развијати специфична култура организације зависи и од многих фактора, а у раду се они групишу у две основе групе:

- утицај који долази из спољашњег окружења: економски, социјални фактори, друштвено-политичко уређење, степен научно-технолошког развоја, безбедносни разлози и други;
- унутрашњи фактори, који између осталих обухватају: мисију, стратегију и технологију организације.

Наше је мишљење да би за будућа компаративна истраживања система заштите информација у различитим географским срединама од значаја било мерити утицај на организациону културу спољашњих фактора.

За безбедносна истраживања унутар организација требало би разматрати унутрашње факторе који чине корпоративну културу. Тако се у посматраном раду наводи да руководство и врховни менаџмент играју велику улогу у дефинисању организационе културе кроз своје поступке и лидерство, а да сви запослени доприносе организационој култури. Руководство организације је заслужно за формулисање и обликовање филозофије организације, што полазећи од нашег предмета истраживања, има пресудну важност и у обликовању безбедносне културе организације.

Што се тиче промена организацине културе, већ је напоменуто да то није процес који траје кратко. Свака организација има јединствену културу, која утиче на брзину промена/иновација. Да би се иновација усталила, неопходно је да је подстичу и прихватају сви запослени и на свим нивоима. Промена се неће укоренити уколико је не прихвати пословодство, или уколико управа не верује у њену вредност, што је нарочито специфично у традиционалним хијерархијским организацијама. Оног тренутка када се прихвати, спровођење и примена се одвијају много лакше и ефикасније него у свим другим институцијама и организацијама у друштву.[96]

Нама су ове констатације које је дала Станаревић од великог значаја за наш предмет итраживања, будући да је заштита информација процес који стално траје и који је потребно стално подизати на виши ниво (због растућих претњи и појаве нових), и која одатле, наше је мишљење, представља у крајњем и део корпоративне културе.

Посебан допринос овог рада је дискусија о контексту културе заштите на раду, односно о контексту културе безбедности и здравља на раду (како слови и Закон који регулише ову област код нас). Наиме, у иностраној теорији и пракси, термини на енглеском језику: *safety* и *security* у доброј мери су дефинисани својим обимом појмовног одређења, тако да се под *safety* подразумевају заштита на раду (некада је ту и против пожарна заштита, а некада она представља посебан појам), а под *security* –

[96] *Ibid.*, стр. 246.

безбедност (физичко-техничко обезбеђење, техничка заштита, интерне истраге и друго).

Станаревић о томе наводи да су сигурност и безбедност појмови сличног значења, у тумачењу подупиру један другог, али ипак постоји разлика која се може уочити управо на примеру концепата које граде, а који наступају упоредо један поред другог – дакле, концепти safety- и security-културе. *Safety* концепт има фокус на ненамерне инциденте (технолошке несреће на пример), док код безбедносне културе (енгл: *security culture*) укључујемо намеру као кључну одредницу према којој је усмерено деловање овог концепта. Безбедносна култура ставља акценат на смишљене поступке, на оне радње које су намеравале да проузрокују штету.[97]

Анализа дефиниција *safety* културе открива да, и поред неуједначености и супротних схватања суштине овог појма, највећи број аутора се слаже у следећем:

- *safety* култура је концепт дефинисан на нивоу групе или вишем нивоу, који се односи на заједничке вредности међу свим члановима групе или организације;
- *safety* култура се бави формалним питањима безбедности у организацији, и блиско је повезана са, али није ограничена, управљањем и надзорним системом
- *safety* култура наглашава допринос свих на сваком нивоу организације;
- *safety* култура организације има снажан утицај на понашање својих чланова на послу;
- *safety* култура се обично рефлектује у непредвиђеном догађају између система награђивања и безбедносних перформанси;
- *safety* култура се огледа у спремности организације да се развија и учи на грешкама, инцидентима и акцидентима;
- *safety* култура је релативно трајна, стабилна и отпорна на промене.

Концепти *safety* културе и *security* културе, закључује Станаревић, у данашњим оквирима представљају управо оне сегменте/димензије корпоративне културе који највише утичу на успех у пословању великих корпорација, оснажујући и доприносећи корпоративној безбедности. У садашњим условима интензивног напретка различитих корпорација и опасности које им прете, јасно је да су култура сигурности и безбедности међусобно повезане и условљене на свим нивоима организационог пословања. Оне заправо све више представљају неопходан услов успешног функционисања безбедносног менаџмента у свим организацијама. У том смислу се и очекује да организације, без обзира на врсту делатности на коју су усмерене, морају обезбедити да ове две културе егзистирају једна поред друге.

Полазећи од предмета нашег истраживања, издвајамо и статове ауторке да успешна промоција безбедносне културе зависи од неколико кључних фактора. Свако лице које се бави безбедношћу организације односно корпорације мора водити рачуна да расправља о случају безбедносне културе на убедљив и кредибилан начин.

[97] *Ibid*., str. 247 – 250.

Континуирана процена безбедносног система, као и способност да се предвиде перформансе система наспрам промењеног сценарија, функција је коју може обављати једино особље које је и само прожето безбедносном културом.

Када запослени не виде да врховни менаџмент доноси јасне изјаве и показује да је безбедност приоритет, неће га ни третирати као приоритет, износи Станаревић. Ова очекивања се односе како на виши тако и средњи менаџмент, вође тимова и супервизоре – где свако треба да прати исту праксу безбедности и процедуре. Јер, ако менаџери не доживљавају озбиљно безбедносну политику или процедуре, ни запослени неће те политике узети озбиљно. [98]

ix. Испитивање односа између организационих система и безбедоности информација

У овом, квантитавином, неексперименталном и корелацијском истраживању, извршеном испитивањем у десет комерцијалних банака на Тајланду, оквир истраживања (однос организационих система и безбедности информација) формулисан је кроз постављање следећих питања: [99]

- какав је однос између структуре организације (где је мерено учествовање у одлучивању и стандардизацији рада) и свести о безбедности информација;
- какав је однос између организационе културе (мерено је организационо лидерство и стил управљања) и свести о безбедности информација;
- какав је однос између политика *HR*-а (мерено је опис послова, провера кандидата, услови запослења, менаџмент одговорности, безбедносна обука) и свести о безбедности информација.

Независне променљиве биле су централизација, формализација, хијерархија, тржишна култура, и правила и политике људских ресурса – *HR*-а (енглески: *Human resource policies and practices – HRPP*). Зависна варијабла била је свест о безбедности информација - ИСА (енгл: *Information Security Awareness – ISA*) корисника.[100]

Централизација се односи на степен дистрибуције моћи у организацији. Перцепција корисника централизације је мерена њиховим учешћем у одлучивању.

Формализација (формализована структура) је независна променљива која одражава степен употребе правила у организацији (ауторитет, одговорност, обавезе и поступци

[98] *Ibid*., str. 326.
[99] Tintamusik, Y.: *Examining the Relationship between Organization Systems and Information Security*, Faculty of the School of Business and Technology Management, Northcentral University, Arizona, USA, 2010.
[100] *Ibid*., str. 9. - 86.

који се морају поштовати, као и контрола примене и правила кажњавања за непоштовање договореног.

Хијерархија као независна променљива односи се на стабилност организационе културе. Главни показатељи су: ефикасност, стабилност и предвидљивост. Ова врста културе је високо формализиована и структуирана описом обавеза радниц места, а лидери су координатори и организатори.

Правила и политике HR-а су независна променљива која утиче на ставове и понашање запослених кроз процесе пре запошљавања (процес селекције у којем послодавац процењује карактеристике кандидата и покушава да утврди његове могућности да током радног ангажовања учествује у смањењу могућности настанка ризика од крађа, превара и злоупотреба). Када је реч о већ запосленима, реч је о напорима организације да олакша процес учења и прихватања правила. Потребно је да су запослени свесни својих одговорности, како би подржали организациона правила током свог ангажовања, услед чега је потребно да имају потребну обуку из области примењивања организационих политика и процедура рада, као и да су упознати са евентуалним дисциплинским потупцима за случај кршења ових правила. Перцепција запослених се мери описом послова, провером кандидата, условима запошљавања, формалном одговорности, безбедносном обуком и познавањем дисциплинских процеса.

Свест о безбедности информација (*ISA*) је зависна варијабла, а односи се на стање где су корисници упознати, свесни и добро обавештени о потребама и начинима заштите информација, као и о последицама које могу наступити (како по организацију, тако и по оне који не поштују прокламована правила). Из тих разлога њима је потребно разумевање, учење, стицање вештина и коришћење стеченог знања – што је пресудно за успех свести о безбедности. Перцепција корисника је мерена кроз посвећеност поштовању дефинисаних смерница и (безбедносних) правила.

Тржишна култура је независна променљива у којој су садржане вредноси које су усмерене на конкурентност, продуктивност и постизање циља организације. Успех ове променљиве се дефинише мерењем тржишног удела организације.

Испитаници су били запослени у десетак комерцијалних банака на Тајланду (банке са страним власништвом капитала су биле искључене из истраживања), који су обављали административне послове, укључујући и оне на руководећим позицијама.

Налази према постављеним истраживачким питањимаод изузетног значаја су за наш предмет истраживања и добијени су према следећем:

Однос између структуре организације (где је мерено учестовање у одлучивању и стандардизацији рада) и свести о безбедности информација. Организациона структура комерцијалних банака обично је умерено централизована, а запослени у пословним банкама су високо свесни информационе безбедности. Постоји слаба и негативна корелација. Да би се повећала зависна варијабла (безбедносна свест

запослених) у овом истраживању, како наводи аутор, потребно је повећати учешће запослених у одлучивању. То се може постићи, на пример, учешћем запослених у спонтаној расправи о неком проблему – брејнстормингу (енгл: *brainstorming*). Аутор наводи да се на овај начин подиже свест о информационој безбедности, што је нама важан став, полазећи од нашег предмета истраживања. На овај начин, подстиче се и ефикасна организација између различитих организационих нивоа. Шта више, учешће запослених у одлучивању (децентрализација) је од суштинске важности за препознавање ризика од сајбер напада у рутинским пословним процесима (јер запослени познају те процесе, наша је примедба). Запослени су највише свесни свакодневних проблема безбедности информација на свом радном месту и других потенцијалних могућности побољшања. Очекује се да запослени могу да идентификују раније познате сајбер нападе, чиме се повећава и свест о информационој безбедности. Знање о идентификованим сајбер нападима ће се пренети међу запосленима и очекује се да ће то довести до побољшања безбедности информација путем безбедносне свести (*ISA*) корисника. Такође, формализација, посматрана кроз експлицитне описе послова, опсежна правила, процедуре и друго, ствара осећај сигурности у организацијама, одакле и она (формализација) доприноси безбедносној свести запослених. Политика заштите информација треба да буде део политике на нивоу целе организације. Није довољно да организација има Програм обуке за повећање свести о информационој безбедности, већ је потребно да се Програм заиста и примењује, како би се осигурало да запослени разумеју изнети садржај.[101]

Однос између организационе културе (мерено је организационо лидерство и стил управљања) и свести о безбедности информација, показује да банке на Тајланду имају тенденцију високе хијерархијске организације и посвећености резултатима. Потврђене су позитивне и умерене корелације посматраних варијабли. Како аутор износи, теорија је већ доказала да је неуспех планираних промена у организацији последица занемаривања организационе културе. Организације све више делују у различитим земљама, одакле захтевају доследност и контролу у процесу пословања. Подизање свести о информационој безбедности (*ISA*) могуће је организовати управо преко организационе културе, као механизма контроле. Када у организацији постоји безбедносна култура, аспекти информационе безбедности се реализују као природан, рутински и свакодневни приступ од стране запослених.[102]

Однос између политика HR-а (мерено је опис послова, провера кандидата, услови запослења, менаџмент одговорности, безбедносна обука) и свести о безбедности информација је такав да постоји умерена и позитивна корелација између њих. Није спорно да запослени могу нанети штету организацији, уколико нису свесни њихове одговорности у том смислу. Руководиоци обе пословне функције треба да сарађују да би произвели политике, стандарде и смернице за информациону безбедност и спречавање сајбер напада. Полазећи од предмета нашег истраживања, нагласили би овај налаз у светлу наших претпоставки да се информациона безбедност не може

[101] *Ibid*., str. 131. – 134.
[102] *Ibid*., str. 134. – 137.

затварати у технички аспект и специфична *IT* знања, већ је потребно да има активну сарадњу са другим пословним функцијама, а пре свега са другим сегментима безбедности. Истраживања која спроводи *HR* могу бити врло корисна за свест о безбедности информација. Такође, и *HR* треба да користи постулате који произилазе из безбедносе културе организације, када организује разговор са кандидатима за посао. *HR* већ у припреми селекцији кандидата може да изврши безбедносну проверу кандидата у смислу провере навода из њихових пријава за посао и испуњености услова за рад на неким радном месту (законитост, пратећи прописи и етика). Запослени треба као део своје уговорне обавезе да потпишу одговорности за поверљивост, заштиту података, етику, одговарајућу употребу опреме и друго. Запослени на (безбедносно) осетљивим позицијама, укључујући запослене у *IT*- у, треба да буду подложни посебним условима запошљавања, као што је провера криминалне прошлости и историје финансијске одговорности код личних плаћања.[103]

x. Како банке поступају у случају безбедносних инцидената на примеру разбојништва – питање кризног менаџмента

Определили смо се за приказ овог рада инспирисани предметом нашег истраживања, будући да аутори у фокус узимају банкарску индустрију и питање функционисања кризног менаџмента приликом избијања инцидената, којом приликом су се одлучили да то учине на примеру избијања разбојништва.[104] У нашем истраживању, навели смо став да је велика група догађаја који се у банкама и финансијским институцијама могу разматрати као безбедносни поремећај, одакле је нарушавање заштите информација само један појавни облик инцидената. Разбојништво, као што су то учинили аутори, може бити друга група безбедносних поремећаја, једнако као што то може бити елементарна непогода, пожар или превара. Сви ови догађаји представљају безбедносне инциденте, и имају како своје специфичности, тако и своја заједничка својства, одакле смо видели везу са нашим предметом истраживања.

Слично нашем претходно изнетом размишљању, аутори износе став да се у банкарској индустрији често расправља о стабилности и сигурности пословања, а кризе представљају све супротно − управо нестабилности и несигурности.

У данашњем глобализованом свету важно је да се организације припреме и организују за потенцијалну кризу. Више није питање како, већ када и зашто се јавља криза, пре питања у којем ће се облику она појавити и колико ће организација бити спремна за њено наступање. Интегрално обележје данашњег информационог доба јесте да се криза више не може видети као ретка и случајна појава, већ се она јавља у све већој учесталости.

[103] *Ibid*., str. 137. – 139.
[104] Andersson, D., Gustavsson, M., Waldén, A.: *How a bank organization handles robberies – a question of crisis management,* Jonkoping International Business scool, Jonkoping University, Sweden, 2008.

Важност управљања кризама први пут је постала препозната када се догодила криза са леком Тиленол 1982. године, а од тада су бројни овакви и слични догађаји који нас упућују на важност управљања кризама и спремности организације за поступање у таквим околностима.[105]

Банке су у погледу „преживљавања" криза изузетно осетљиве, јер неприпремљеност на кризу (па и кризе изазваних безбедносним инцидентом) има утицај и на клијенте, од чијег поверења зависи пословање. Од банке, односно од финансијске институције, очекује се стабилност и поузданост. Традиционално, људи поклањају поверење банкама јер су решили да им повере свој новац, односно да преко њих обављају своје финансијске трансакције, јер је опет банка место где ће новац бити сигуран. Када се овај механизам поверења распадне, што може да се догоди у кризи изазазваној безбедносним инцидентом, клијенти се налазе пред избором да ли и даље да верују својој банци или да потраже неку другу. Криза дакле доводи у питање претпоставке стабилности и поузданости, а карактеришу је нејасноћа, несигурност и нестабилност. Када се банка суочи са кризом, поновно успостављање репутације и обнове поверења мора бити питање свих питања управа банака.[106]

Аутори у раду одређују основна истраживачка питања трагајући за одговорима: како је организовано управљање банкама у кризним ситуацијама, и – колико је важан поглед јавности на безбедност банке (у случају разбојништва, иако смо претходно објаснили однос према нашем предмету истраживања).

Средином прошло века (завршетком II светског рада), компаније су имале захтев према осигуравајућим кућама да се смање осигуравајуће премије у доба мира који је наступио. Како ови захтеви нису били услишени, организације су покушале да смање

---

[105] Криза је наступила када је умрло седам особа које су користиле лек Тиленол (енгл: *Tylenol*, најпознатији аналгетик у САД, произвођача Johnson & Johnson), пошто је неко успео да убаци једну малу, али смртоносну количину цијанида у лек. Нико није знао у којој мери је лек контаминиран, а опасности је било изложено око сто милиона американаца који су користили Тиленол. Кључну улогу у упознавању јавности са опасности имали су медији. Тровања су захтевала хитну акцију, а прва важна одлука Џонсон и Џонсона је била да се буде апсолутно отворен према јавности. Лек је очекујуће повучен из продавница широм земље. Са аспекта управљања кризама, компанија је поступила заправо према креду који је формулисао син власника, директор, Роберт Џонсон, још далеке 1943. године. Према том постулату, четири су основна аспекта одговорности који има компанија: најважније је одговорност према потрошачима, следи одговорност према запосленима, па према друштвеној заједници, а тек на крају је одговорност према акционарима. Одмах је формиран одбор за реаговање према медијима, који су чинили највиши руководиоци управе. Организован је огроман број конференција за штампу и на крају телевизијска кампања која је покривала целу Државу. После шест недеља, анкете су показале д а чак 90% американаца није кривило произвођача за инцидент, а да је 80% становништва било спремно да поново купује Тиленол. Нешто касније, продаја овог лека је забележила огроман пораст. Четири године касније, још једна жена је умрла користећи овај лек. Поступање Џонсон и Џонсона се поновило као приликом избијања прбог инцидента. Од тада, компанија је објавила да неће рекламирати производе који се не издају на лекарски рецепт и тог правила се придржавају и данас. Продаја Тиленола је поново порасла. Више у чланку: Улога односа са јавношћу у решавању кризе са леком Тиленол, доступно на: : http://aleksisdimy.blog.rs/blog/aleksisdimy/generalna/2011/10/12/uloga-odnosa-s-javnoscu-u-resavanju-krize-sa-lekom-tylenol

[106] D. Andersson, M. Gustavsson, A. Waldén, *op.cit*., стр. 2.

ризике са којима су суочене. Након неког времена бављења овом проблематиком, специјалисти за питања смањења ризика су означени као „менаџери ризика“. Осемдесетих и деведестих година управљање ризиком је развило методе идентификације и елиминације ризика, где је примену нашла наука, а посебно вероватноћа, да би данас говорили о управљању ризиком као пословном функцијом у којем се он идентификује, мери, надгледа и где се преузимају различите радње за управљање (исто тако различитим) ризицима.

У банкарској индустрији криза је увек присутна, па је и управљање кризама од великог значаја. Тако аутори износе различита теоријска тумачења концепта кризе, где између осталог наводе да је организациона криза догађај мале вероватноће који има висок утицај који прети одрживости организације и догађај где се мора поступати брзо. Исто тако, наводе и да уколико целокупни процес стратешког планирања не укључује управљање кризама је исто као одржавање живота без гарантовања живота. [107]

Посебан допринос нашем предмету истраживања, пронашли смо у разматрању типологија криза у научној теорији, како су то дали аутори овог истраживања.

Они наводе да постоје три различите врсте кризе: криза у континуитету, криза у настајању и непосредна криза. Она може трајати недељама, па чак и годинама и често се у овим случајевима ради о спекулацијама, трачевима и гласинама (криза у континуитету). Криза у настајању је спора, али често је код ње тешко саставити све делове, како би се предвидео долазак кризе. Фокус њиховог рада је на непосредној кризи која менаџерима пружа мало или нимало упозорења. Тешко је или чак немогуће предвидјети ову врсту кризе, али важност добро припремљености је од суштинске важности за непосредни кризни сценарио – какав је случај код оружаног разбојништва.

Аутори наводе Митрофову типологију криза према дејству следећих фактора:[108]

- *економских*, када се догађа пад на тржишту, услед непријатељска деловања конкуренције и друго;
- *информационих*, која се јављају лажне информације, долази до губитка података, онеспособљавања информатичких ресурса и друго;
- *физичких разлога*,када долази до губитка кључне опреме, кварова производа и друго;
- *HR узрока*, када долази до губитка кључног особља, корупције, насиља на радном месту и друго;
- *нарушавања угледа*, када се јављају трачеви, гласине, наноси штета општем угледу и друго;
- *деловања криминалних радњи*, као што је отмица, тероризам, кривична дела и друго;

[107] *Ibid*., стр. 4. – 5.
[108] *Ibid*., стр. 6., аутори се позивају на налазе: I. Mitroff, *Managing Crisis Before They Happen: What Every Executive and Manager Needs to Know about Crisis Management.* New York*:* Amacom, 2000.

– *деловања природних катастрофа*, услед дејства поплаве, пожара, земљотреса и сл.

Извор на који се претходно позивају аутори истиче важност психолошког аспекта управљања кризама и припреми кризе када се она још није догодила. Организације, слично као и појединци, постављају одбрамбене механизме како би онемогућили и негирали своју рањивост. Тако је Митроф препознао различите врсте одбрамбених механизма који могу постојати у култури организације (и који су блиски са Фројдовом теоријом одбрамбених механизама):[109]

– порицање (криза се дешава другима, наша организација је нерањива);
– омаложавање (кризе се догађају, али ако и погоди нашу организацију, утицај ће бити мали);
– идеализација (криза не погађа добре организације, као што је наша);
– величање (наша организација је тако велика, па ћемо бити заштићени од кризе);
– пројекција (ако се и догоди криза, то је зато што је неко то желео да се догоди);
– интелектуализација (вероватноћа да се догоди је мала);
– парцијализација (ако се догоди криза, не може да утиче на целу организацију).

Реч је дакле о механизмима које организација мора да препознаје и да се бори против њих, будући да се у свим овим случајевима запоставља реалан контекст који може наступити деловањем кризе.

Банкарска организација треба да препозна различите фазе кризе, а проблем се усложњава чињеницом да се криза ретко када догоди како је то организација планирала. Из тих разлога важно је бити флексибилан и прилагодљив у припремама за кризу. Аутори тим поводом наводе Митрофов модел, који је настао побољшањем његовог провобитно тростепеног модела, моделом који је касније развио у сарадњи са Паучантом (енгл: *Pauchant*) и који садржи пет фаза, према следећем:[110]

Схема број 3: ***Комбиновани модел управљања кризом према Митроф и Паучант***

ФАЗА 1: ПРЕ КРИЗЕ	ФАЗА 1 и 2: (1) ОТРИВАЊЕ КРИЗЕ *(2) ПРИПРЕМА И ПРЕВЕНЦИЈА*
ФАЗА 2: ЗА ВРЕМЕ КРИЗЕ	ФАЗА 3: (3) ОГРАНИЧАВАЊЕ ШТЕТЕ
ФАЗА 3: ПОСЛЕ КРИЗЕ	ФАЗА 4 и 5: (4) ОПОРАВАК И *(5) УЧЕЊЕ*

[109] *Ibid*.
[110] *Ibid*., стр. 7.

Раније смо напоменули да безбедносни инциденти, имају како своје специфичности, тако и своја заједничка својства.

Мишљења смо да, иако је у посматраном раду реч о оружаним разбојништвима, треба напоменути да фаза откривања, припреме и превенције, јесте различита у смислу предвиђања када ће се она и где догодити. Са друге стране, није ограничавајући фактор да се банка припреми на овакву кризу, посебно кроз анализу зашто би се дело догодило баш ту (у односу на друге банке у окружењу). Чак је предвидљив и податак када би се дело могло догодити (вероватноћа да ће се догодити је тада већа него у другим околностима), па тако организација може да разматра податке када су се и колико често догађала таква дела у окружењу (статистички је могуће одредити учесталост догађаја: којим данима у недељи, у које доба дана, да ли је у другим случајевима било у објекту других клијената, да ли је особље објекта познаје своје клијенте итд.), када је у банци највише новца, какве су процедуре за интерни трансфер новца од трезора до благајни и друго.

Фаза ограничавања настале штете подразумева да је догађаја већ дошло, па се у овој етапи разматрају механизми којима банка располаже да нападачима буде доступно што мање новца, а да се са друге стране не провоцира даља употреба силе и већи степен насиља.

Завршна фаза, подразумева да се безбедносни инцидент већ догодио и предвиђа на који начин банка може да се што пре оспособи за редовно пружање услуге својим клијентима. То не спречава, на против, анализу насталог догађаја и посебно – учење организације како да убудуће унапреди почетну фазу, октривање кризе и припрему и превенцију штете (евалуација стечених знања).

Банка, кроз овај модел може управљати кризом и за другу врсту догађаја, што се свакако односи и на инциденте који спадају у нарушавање система заштите информација.

Ми се, полазећи од предмета нашег истраживања, нећемо детаљније задржавати на даљим анализама аутора, али сматрамо да је корисно за будућа истраживања из области коју рад третира напоменути да се у раду разматрају и питања формирања Тима за поступање у кризи, питања руковођења за време кризе, а посебно да су аутори аргументовали њихов методолошки приступ истраживању безбедносних инцидената (инструмент је био полуструктуирани интервју) и да су том приликом препознали евентуална ограничења у вези са поверљивошћу разматраних информација и начине како би се овај проблем могао превазићи.

На крају, истакли би као користан за будућа истраживања један од закључака истраживача који се односи на планирање истраживачког поступка, где они наводе да је слаба повезаност интерних сазнања банака о безбедносним инцидентима и полиције, будући да су банке занемариле чињеницу да полиција поседује велико знање о предметној области и да је експерт за кризне ситуације као што је ова посматрана. Из тих разлгога будућа истраживања треба да укључе и полицију, као и струковне организације, у већој мери, а не да су ограничена само на особље банака.

Банке би морале да буду отвореније према полицији са својим политикама и да на тај начин омогуће себи повратна сазнања која ови имају. Аутори верују да би таква сарадња допринела бољој припремљености организација за руковођење у кризама, а посебно у инцидентима који се односе на преваре и разбојништва. Један од испитаника је учествовао на семинару који је организовала полиција, где су учешће узеле и особе које су биле присутне током извршења дела разбојништва, где су ови поделили шта су осећали и доживели када се ово дело догађало. Истраживачи верују да би овакви семинари користили запосленима у банци и да би то био још један допринос припремљености организације за кризне ситуације изазваним безбедносним инцидентом као што је оружано разбојништво.

xi. Десет смртних грехова информационе безбедности

Овај научни рад[111] нам је привукао пажњу полазећи од предмета нашег истраживања, а посебно узимајући у обзир респектабилну каријеру аутора у области заштите информација.[112]

Аутори износе аспекте који су по њиховом мишљењу незаобилазни у изради безбедносе стратегије у компанијама, односно представљају оквир који је потребно дискутовати да би већ постојеће стратегије побољшале своју ефикасност.

У раду се наводи да изостављање било којег од наведених аспеката неминовно има за резултат неконзистентност у спровођењу заштите информација у организацији, одакле ћемо приказати њихове налазе, и то:

1. Информациона безбедност је одговорност највиших управљачких структура
2. Информациона безбедност је приоритетно пословно а не технико питање у организацији
3. Информациона безбедност захтева мултидисциплинарни приступ

---

[111] Solms, B., Solms, R.: *The 10 deadly sins of information security management,* Computers & Security, No. 23, 2004., pg. 371. – 376., доступно на: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v10/learningdocs/VonSolms-10-Deadly-Sins.pdf

[112] *Basie von Solms*, је професор на Академији за рачунарску науку и софтверски инжењеринг на Универзитету у Јоханесбургу, Јужна Африка. У тамошњим научним и стручним круговима се сматра за „оца информатичке сигурности“, а његове области рада су безбедност информација и сајбер безбедност. Тренутно је директор Центра за кибернетичку безбедност на Универзитету у Јоханесбургу, као и придружени директор Глобалоног центра за кибернетичку безбедност Универзитета Оксфорд. Од 2018. године, члан је Глобалног савета за сајбер безбедност Светског економског форума. Аутор је више од 150 радова из наведених области, који су углавном публиковани у међународним стручним издањима. Руководио израдом више од 120 постдипломских радова, из области информационо комуникационих технологија (ИКТ-а), што укључује готово 30 докторских радова. Доступно на: https://adam.uj.ac.za/~basie/biography.html#focus. *Rossouw von Solms,* South African Institute Computer Scientists and Information (board directors), доступно на: https://www.saicsit.org/

4. План информационе безбедности мора се заснивати на утврђеним ризицима
5. У информационој безбедности је потребно примењивати искуства најбоље праксе
6. Безбедносна Политика заштите информација је неоходна (документ)
7. Спровођење и надгледање безбедносне праксе у заштити информација је неопходно у организацији
8. Управљање пословима безбедности информација је неопходно у организацији
9. Информисање о безбедности информација је неопходно у организацији
10. Недавање подршке информационој безбедности потребном инфраструктуром и алатима

Информациона безбедност је одговорност највиших управљачких структура, је теза која је ослоњена на настанак неколико докумената у свету који регулишу област корпоративног управљања и приватности одређених информација, као и обавезе оних којих их нарушавају. У том смислу аутори наводе неколико примера, као што су *COBIT*[113] и *HIPAA*[114]. Импликација ових дешавања је та да највише руководство (на пример Управни одбор) имају директну одговорност за корпоративно управљање у погледу заштите свих поверљивих информација компаније. Компромитовани информациони ресурси могу имати озбиљне финансијске и правне импликације на компанију и извршно руководство, а некада се та одговорност своди и на личну одговорност. Такође, обавеза извршног руководства је да извештава (управни Одбор) о заштити информационих средстава.

Информациона безбедност је приоритетно пословно а не технико питање у организацији, што извире из претходно наведеног о одговорности највиших управљачких структура. Аутори наводе да се проблеми који се односе на информациону безбедност не могу решити (само) техничким средствима. На жалост, настављају Солмс и Солмс, у многим случајевима извршно руководство у компанијама и даље мисли да је ово техничко питање (а ми би додали, полазећи од нашег предмета истраживања, да и даље мисле да се заштита информација суштински своди на *IT* активности обавезе). Последица чињења овог греха је да се безбедност информација своди на технологију.

Информациона безбедност захтева мултидисциплинарни приступ, што поново извире из претходно изнетог о фокусу на пословно а не техничко питање. Безбедност

[113] *Cobit* је међународно прихваћен стандард у којем се прописују подручја и појединачне контроле за корпоративно управљање информатиком и припадајућим информатичким ресурсима. Он спаја пословне и информатичке циљеве пружајући могућност да се метрички прати зрелост информационог система. Више о томе: *Анализа концепта ревизије информационих система према Cobit методологији*, Милован Станишић, Далибор Радовановић, Дубравка Лучић, 6. Научни скуп са међународним учешћем Синергија 2010., Универзитет Синергија, Бијељина, Република Српска, стр. 154. – 161.

[114] *The Helth Insurance Portability and Accountability Act (HIPPA)*, правила садрже захтеве о приватности, безбедности и обавештењу о кршењу који се примењују на појединачне идентификационе здравствене податке које креирају, примају, одржавају или преносе пружаоци здравствених услуга који обављају одређене електронске трансакције, здравствене трансакције , здравствене планове, канцеларије за заштиту здравља и њихове пословне сараднике. Доступно на адреси: https://www.hhs.gov/foia/privacy/index.html

информација је вишедимензионална дисциплина и све димензије се морају узети у обзир да би се осигурало безбедно окружење за информатичке ресурсе компаније. Аутори се позивају на објављену литературу, али и на обављене разговоре са руководиоцима информационе безбедности. Они износе став да листа, како су је дали у овом раду, није коначна, као и да се неке димензије могу преклапати у погледу њиховог саржаја. Коначно, важна је идеја о мултидисциплинарности, а не број и садржај димензија, које су дате према следећем:

- димензија корпоративног управљања;
- организациона димензија;
- димензија политике;
- димензија најбоље праксе;
- етичка димензија;
- димензија цертификације;
- правна димензија;
- димензија осигурања;
- особље / људска димензија;
- димензија свести;
- техничка димензија;
- мерење / метрике (надгледање усклађености / *IT* ревизија у стварном времену);
- димензија ревизије.

Уочљиво је, истичу аутори, да је већина димензија нетехничке природе, и да се оне морају све узети у обзир приликом израде свеобухватног плана информационе безбедности предузећа. Последица овог греха је стално враћање на процес планирања, јер ће се у пракси увек јавити недоследности и нелогичности.

План информационе безбедности мора се заснивати на утврђеним ризицима, јер сврха информационе безбедности јесте управо пружање мера за ублажавање ризика који су повезани са информационим ресурсима компаније. Солмс и Солмс тако наводе да ако компанији није јасно шта су потенцијалне претње, као и која се имовина штити, слично је као и „пуцати у мраку“ и трошити новац на нешто што су претње које су врло ниских вероватноћа и којом приликом се занемарују оне претње које имају велики утицај. Од суштинске је важности да компанија свој план безбедности информација заснива на некој врсти вежбе анализе ризика. То може бити структуирана и свеобухватна вежба, у комбинацији са примерима најбоље праксе. Последица чињења овог греха је да компанија троши новац на ризике који не представљају велику опасност, а да са друге стране игнорише оне „праве“ ризике.

У информационој безбедности је потребно примењивати искуства најбоље праксе, јер типична питања за којима менаџери безбедности информација трагају јесу: Од којих ризика се штитимо и који би то сет контра мера одговарао претњама. Ова питања морају имати своје одговоре, у супротном компанија може трошити новац на непотребне и неефикасне против мере. Концепт примене најбоље праксе је заснован

на идеји учења из искуства других, јер је велики проценат претњи безбедности информација и изабраних контра мера исти за све компаније. Аутори се питају зашто би понављали оно што су други већ учинили („зашто поново измислити точак“ они наводе). То нас међутим доводи до следећег питања: како да менаџер за безбедност информација зна које су то „праве ствари“ које је потребно применти у његовом пословном окружењу. Одговор се крије у претходном искуству струке, који се у основи називају стандарди и смернице. Ови извори се требају посматрати као консензус стручњака за поље информационе безбедности. Са друге стране, изнети ставови не значе да се примери најбоље праксе морају нужно применити, већ предузимање конкретних мера зависи и од конкретних околности. Примери водећих најбољиих пракси у области информацијске безбедности дати су кроз Стандард ISO 17799[115]. Ми би овоме додали и Стандард ISO 27001, који аутори нису овде уврстили због чињенице да су рад писали пре доношења стандарда.[116]

Безбедносна Политика заштите информација је неопходна, којом приликом аутори мисле на документ који регулише ову област. Политика је полазна основа од које потичу све под политике, процедуре и друга нормативна документа. Политика заштите информација треба бити кратка (три до четири странице текста) и потисана од стране највишег директора у хијерархији организације, чиме се показује посвећеност руководства свим аспектима информационе безбедности. Ово је и највидљивији начин на који управа организације показује своју посвећеност информационој безбедности. Последица чињења овог греха би била да сви пројекти информационе безбедности и други напори компаније у том смислу, немају сидриште и доказ своје посвећености наведеном.

Спровођење и надгледање безбедносне праксе у заштити информација је неопходно у организацији, будући да нема смисла имати чак и савршену корпоративну политику безбедности информација, са свеобухватним сетом под политика и процедура, усаглашених са најбољом праксом, ако није могуће надгледање и контрола примене донетих прописа. С тим у вези, менаџер за безбедност информација треба да је опремљен техничким и нетехничким алатима за мерење предметног садржаја, као би могао да надгледа поштовање релевантних политика, те да поступа према одговарајућим налазима ако уочи неусаглашености. Такви алати за надледање и мерење морају да се третирају у извештајима Интерне ревизије (чиме се остварује још једна контрола која је у функцији заштите информација у организацији, наша је

[115] Стандард ISO 17799 даје препоруке најбоље праксе за покретање, примену или одржавање система управљања сигурношћу информација. Сигурност информација је дефинисана у стандарду као очување поверљивости (да информације буду доступне само онима којима је дозвољен приступ), интегритет (заштита тачности и потпуности информација и метода обраде) и доступност (да овлашћени корисници имају приступ информацијама и другим средствима када су она потребна). Више о *ISO* 17799 доступно на: https://www.bankinfosecurity.com/iso-17799-27001-setting-standards-for-information-security-a-165

[116] Стандард ISO 27001 одређује захтеве за успостављање, примену, одржавање и унапређење система управљања сигурношћу информација у складу са најбољим праксама описаним у ISO 17799. ISO 27001 је формални стандард за који организације могу тражити независну сертификацију својих система управљања сигурношћу информација. Више о стандарду доступно на: https://www.bankinfosecurity.com/iso-17799-27001-setting-standards-for-information-security-a-165

примедба), јер како наводе аутори, нико више нема луксуз да после шест месеци, на пример, утврди да запослени који је напустио компанију има и даље активне привилегије после толико времена (мисли се на привилегије за приступање систему, информацијама и слично). Такви алати морају пружати податке о мерењу (и извештавање) у реалном времену. Како наводе аутори, можете управљати само са оним што можете мерити. Последица чињења ово греха је пружање лажног осећаја сигурности, јер и ако организација има све неопходне политике она можда и не зна да оне заправо не постоје.

Управљање пословима безбедности информација је неопходно у организацији, је неопходно, што је нагласило и неколико кодекса најбоље праксе за управљање информационом сигурношћу. Ово укључује и формирање посебних Одбора за информациону безбедност, што би требало да буде место где се сусрећу различити аспекти у заштити информација организације и где учешће узима највиши менаџмент. Одбор треба да утврди и које аспекте управљања информацијском безбедношћу је потребно централизовати, а које аспекте треба децентрализовати, као и где се обавља надзор над применом прописаног. Аутори напомињу да се надгедање никада не треба организовати у *IT*-у (јер би на тај начин контрола била у сукобу интереса са овом пословном функциојом, наша је примедба). Последица чињења овог греха: све што је повезано и укључује информацијску безбедност аутоматски се упућује менаџеру безбедности информација, који заиста није власник свих информација. Ако власници информација ниу дефинисани, а по природи ствари они јесу одговорни за сигурност информација под њиховом контролом, настају озбиљни безбедносони ризици. Одговорност за безбедност информација деле сви запослени, у складу са претходно наведеним, а не само менаџер за информациону безбедност. Ова одговорност мора бити дефинисана (одређивање власника информација), написана и смештена у одговарајуће организационе структуре.

Информисање о безбедности информација је неопходно у организацији, што на први поглед може изгледати као тврња коју не треба посебно доказивати, али у пракси се може приметити да поједине организације и даље праве овакву грешку, износе аутори. Не постоје одговарајући програми развоја безбедносне свести (енгл: *security awareness*) па корисници нису свесни ризика који доноси *IT* инфраструктура. То значи и да корисници нису свесни постојања безбедносне политике и пратећих процедура, за шта они (корисници) не могу да сносе одговорност, јер им није ни речено какви су безбедносни проблеми и шта они треба да чине да спрече настајање штете. Солмс и Солмс наводе да је новац који се троши за програме развоја свести о безбедности информација можда најбоље потрошен новац у компанији. Последице чињења овог греха: безбедност информација у компанији неће успети ако се корисници не едукују о политици безбедности, могућим претњама и начинима њиховог доброг поступања у смислу превенције штетних догађаја.

Не давање подршке информационој безбедности потребном инфраструктуром и алатима, је уско повезано са одсуством управљања и информисања у обој области, што су аутори изнели образлажући претходне две грешке коју могу да чине

организације, али се због своје важности издваја као посебна грешка. Често извршно руководство успостави фукцију безбедности информација (у неком облику) и очекују да су на тај начин решили ово важно питање. То није могуће у пракси, полазећи од сложености и вишедимензионалности информационе безбедности. Последица ове грешке (греха, како износе аутори) јесте да менаџери информационе безбедности после неког времена схватају да не могу правилно обављати свој посао и увиђају узалудност пословне функције за коју су задужени. На овај начин, отварају се врата компаније за озбиљне ризике, јер се у коначном нико у организацији не бави заштитом информација.

Солмс и Солмс на крају наводе да је пратећи листу „грехова“ у информационој безбедности, како су је навели у овом научном раду, лако доћи до одговора да ли је организацији неопходна ревизија безбедносне политике у заштити информација. Довољно је да макар и један одговор на овако формулисана питања буде негативан.

xii. Успостављање организационе културе информационе безбедности у организацијама: приступ на основу едукације

Аутор у овом раду полази од поставке да је избегавање губитака или оштећења информационих ресурса императив којим се компаније активно баве.[117] У том смислу постоји велики број контрола, али је тешко одредити које су то активости, да би се гарантовао минимални ниво безбедности. Овај проблем је још сложенији, будући да су се развојем интернета и електронског пословања компаније ставиле у позицију да морају да воде рачуна и о безбедности својих партнера у пословању, а не само да посматрају сопствене ресурсе. Из тих разлога, управљање безбедношћу информација представља велики изазов и може да се постигне само уз помоћ холистичког приступа који је заснован на међународним стандардима.

Један од значајних стандарда, из перспективе времена писања овор рада и полазећи од предмета истраживања, јесте стандард ISO 17799, који смо претходно и сами спомињали у нашем истраживању и који даје препоруке најбоље праксе за покретање, примену или одржавање система управљања сигурношћу информација. Једна од кључних активности јесте увођење програма о безбедносној свести у заштити информација, где је суштина у едукацији корисника о појединачним улогама које они имају у остваривању овог система.

---

[117] Niekerk, J. F.: *Establishing and information security culture in organizations: an outcomes based education approach*, Dissertation submitted in fulfillment of the requirements for the degree Magister Technologiae in Information Technology, Faculty of Engineering, Nelson Mandela Metropolitan University, University in Port Elizabeth, South Africa, 2005.

Прегледом релевантне литературе, аутор износи став да се контролне активности безбедности информација могу поделити у три групе, наводећи их према следећем:

- физичке контроле, које представљају физичке аспекте безбедности, где на пример, ова функција може навести да канцеларија која садржи осетљива документа треба да има организовану контролу приступа;
- техничке контроле, где се корисници могу присилити да се аутентификују јединственим корисничким именом и лозинком пре приступања информационом систему организације;
- оперативне контроле, које се састоје од свих контрола које се баве људским понашањем, а што представља највећу претњу безбедности информација и упућује на закључак да је овде реч о најслабијој карици у остваривању овог вида заштите.

Аутор примећује да се и физичке и техничке контроле ослањају на оперативне контроле, па се тако може догодити да корисници игноришу правила ових функција (да ли из незнања или из намере), што обесмишљава читав систем заштите (на пример: правила да се приликом изласка из канцеларије корисник мора да излогује из система и да за собом затвори/закључа врата канцеларије, неће ништа вредети уколико корисник не поступи тако), и тада је реч о илузији безбедности.

Развој безбедносне свести дакле представља круцијални елемент заштите, па се даље поставља питање на који начин приступити овој активности у организацији. Никерк у свом раду износи становиште, засновано на дотадашњим теоријским истраживањима, да је добра околност да постоје стандарди и смернице које упућују организацију на потребу организовања обуке за информациону безбедност, али исто тако и да су оне начелне и да не дају одговор на питање шта је то одговарајућа обука.[118]

Аутор наводи да стандарди занемарују одговарајуће образовне принципе, што се усложњава чињеницом да програме за развој безбедносне свести формирају углавном IT професионалци, који немају потребна знања како је наведено. Постоје и неколико других фактора који утичу на неефикасност програма за подизање свести, као што су:

- садржаји програма су једноставни, одакле постоји могућност да постану монотони слушаоцима;
- мање од 25% генералних директора сматра безбедност информација важном пословном функцијом;[119]
- садашњи програми су неадекватни, недовољно свеобухватни и углавном се односе на крајње кориснике;
- садашњи програми не обраћају пажњу на теорије понашања.[120]

[118] *Ibid*, стр. 2. – 4.

[119] Никерк се позива у овој тврдњи на извор: *The development of an effective information security awareness program for use in an organization.* Thomson, M., Master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa, 1998. Година, стр. 17.

[120] Никерк се позива у овој тврдњи на извор: *Five Dimensions of Information Security Awareness,* Computers and Society, M.T. Siponen, 2001., стр. 24. - 29.

Полазећи од значаја безбедности информација, овакви програми морају превазићи наведене примедбе и околности, не губећи при томе из вида да није реч о формалном образовању, већ о припреми корисника за одговарајуће безбедносно понашање у организацији.

С тим у вези, аутор износи став да би у образовању одговарао приступ који сваки део образовног система заснива на циљевима (енгл: *outcomes-based education − OBE*).[121]

ОБЕ приступ у ствари може бити идеалан за употребу у програмима, с обзиром да циљ није припремити полазника за испит или за даљи ниво формалног образовања, већ управо има функцију да помогне полазницима да постигну конкретан циљ, у нашем случају – свест о информационој безбедности.

Никерк наводи у свом раду да у теорији нема знања о погодности ОБЕ-а за креирање корпоративних образовних програма у информационој безбедности. Он је овај проблем видео као двострук, и то:

- безбедност информација зависи од људи који су укључени у процес заштите информација, а тренутни програми не придају довољно пажње теоријама понашања. Едукација заснована на резултатима је педагошка методологија која би могла бити погодна за стварање информационе сигурности;
- неговање организационе субкултуре безбедности информација је неопходно у организацији. У теорији је добро проучен проблем промене корпоративне културе, али је недовољно проучен процес промене субкултуре заштите информација.

Аутор наводи и да, у време писања његовог рада, постоји модел обуке о безбедности информација издат од стране америчког националног института за стандарде и технологију (енгл: *NIST 800-16*).[122] НИСТ модел је заснован на претпоставци да је учење континуитет. Учење у овом контексту почиње са свесношћу, надограђује се на обуку и развија у образовање. Заснива се на игрању улога, што у пракси значи да полазници прођу више различитих улога у организацији (са различитим одговорностима) у вези са информационим системима. Претпоставка је да је учење информацине безбедности процес у континуитету, те да се састоји од развијања свести о безбедности, тренинга и едукације, према следећем:

[121] ОБЕ је теорија образовања која сваки део образовног система заснива на циљевима (исходима). На крају образовног искуства, сваки је ученик требао постићи циљ. У ОБЕ нема одређеног одређеног стила предавања или оцењивања; Уместо тога, часови, прилике и оцене треба да помогну ученицима да постигну задане исходе.

[122] Стандард је издат под називом: *Захтеви за обуку у области информационе технологије, засновано на моделу уога и перформанси* (енгл: Information Technology Security Training Requirements: A Role- and Performance-Based Model), више о томе, Niekerk, J. F, *op.cit*., стр. 30. – 32.

- свест о безбедности информација (енгл: *security awareness*), полазник је прималац информације и не учествује активно;
- тренинг, полазник мора знати како се треба безбедно понашати у контексту теме обуке. Овај ниво тежи да развије потребне безбедносне вештине;
- образовање, уједињује безбедносне вештине игране у различитим улогама у заједнички корпус знања. Успешан је када корисник на крају зна одговор на питање зашто је потребно понашати се на безбедан начин.

Начелно, организације треба да прилагоде своје програме за развој свести о безбедности на такав начин да уваже своје конкретне потребе и структуру запослених (профил радне снаге, опис њихових послова, интерну организацију рада, старосну и образовну структуру, њихово радно искуство и друго). Како се у организацијама по правилу ради о одраслој популацији, потребно је уважити и педагошка правила која важе за образовање одраслих.

Аутор је предложио критеријуме које би овакви програми требало да испуњавају, и то:

- сви полазници треба да буду у прилици да „прођу“ тренинг;
- запослени треба да разумеју због чега су им потрене вештине које уче, односно због чега треба да се понашају на одређени начин;
- материјале за учење треба прилагодити стилу учења;
- полазници треба да су одговорно за своје учење;
- полазници треба да добију повратне информације о успешности обуке.

Концепт корпоративне културе је свакако важан (ако не и одлучујући, наше је мишљење) за спровођење информационе безбедности у организацији. Никерк наводи да се овим механизмом утиче на ставове запослених о исправности понашања које подразумеба информациона безбедност. Он наводи налазе теорије, да се корпоративна култура састоји од три нивоа, и то:

- артефаката: видљиво и мерљиво свакодневно понашање запослених;
- прихваћених вредности: писани документи који подржавају формалне вредности организације;
- заједничких прећутних претпоставки: то су прави покретачи понашања запослених и настају као резултат заједничког учења и искуства.

Сваки покушај промене корпоративне културе (дакле и субкултуре која се односи на информациону безбеност) мора да се бави заједничким прећутним претпоставкама. Овај ниво се састоји од веровања, вредности и принципа које гаје запослени. Проширење концепта промене корпоративне културе, када је у питању заштита информација, подразумева и потребна знања која је потребно да запослени усвоје.[123] Ставови и знања запослених у информационој безбедности зависе један од другог.

[123] Niekerk, J. F, *op.cit*., стр. 75. – 76.

Теорија организационог учења, наводи аутор, није сама по себи довољна за промену корпоративне културе организација, већ је потребан формализовани процес управљања променама који долази из менаџерских наука. Било који покушај промене заједничких прећутних претпоставки, уколико није спроведен на одговарајући начин, могао би да резултира психолошком анксиозношћу међу запосленима. Ови психолошки фактори у раду су укратко представљени, а ми ћемо их, полазећи од значаја за предмет нашег истраживања навести, према следећем:

- страх од казне за неспособност; запослени могу да се плаше да троше превише времена за учење „новог начина ствари“, услед чега га никада неће ни научити;
- страх од губитка личног идентитета; запослени се одупиру променама јер сматрају да је „стари“ начин био сасвим добар и да су га они добро обављали. Пример за овакав страх аутор наводи кроз промене које доноси превенција социјалног инжењеринга. Запослени који је увек би „ту за све“ не жели да буде друга особа, јер се од њега сада очекује да буде опрезан према свима који му прилазе и од њега захтевају „нешто“, како би препознао сумњиво понашање;
- страх од губитка чланства у групи; заједничке прећутне претпоставке упућују запослене да одреде ко је „унутра“, а ко „изван“ група. Ако се људи мењају, плаше се да ће их њихова постојећа група одбити из свог окружења.

Аутор је покушао да представи холистички оквир за увођење организационе субкултуре информационе безбедности, прем којем је изнео следеће:

Обавезе највиших руководећих структура („топ“ менаџмента) је да покаже своју искрену посвећеност безбедности информација, и то не само декларативно (али и на тај начин), већ и сопственим примером. Они ће награђивати „ново“ понашање, а кажњавати „старо“. Ове промене мора пратити и нова Политика безбедности заштите информација, односно одговарајуће подполитике, а свака се бави специфичним аспектима жељене културе.

Дефинисати проблем у пословном контексту, подразумева да се сваки појединачни проблем посебно третира, а да је том приликмо неопходно проценити тренутно стање, где организација променом жели да дође, и – на који начин постићи жељени циљ.

Едуковати запослене по некада подразумева да запослени одбијају потребу за новим, одговорним обрасцима понашања. То траје толико дуго, док им се не објасне опасности за безбедност информација (на пример док им се не објасни потреба за увођењем јачих лозинки за логовање на информациони систем). Аутор тако наводи да није довољно да запослене научимо шта да раде и како то да раде, већ је потребно да разумеју и зашто то раде.

Дефинисати мерење у промени културе је потребно да би запослени имали повратну (квантитативну) информацију о успешности изведене промене у њиховом понашању, а затим и у самој организацији. Треба имати на уму да су заједничке прећутне претпоставке резултат континуираног понашања у прошлости, као и да некада може

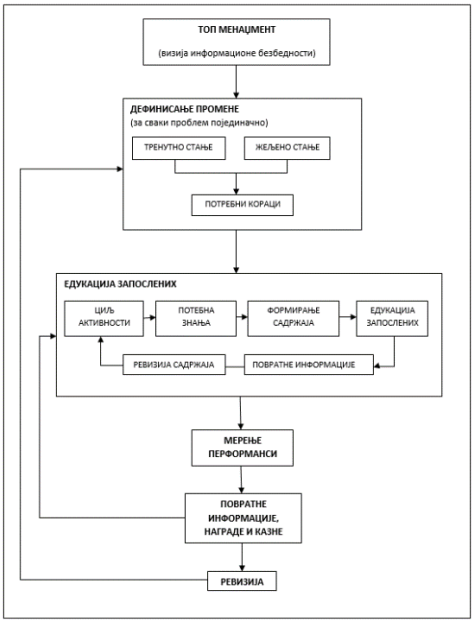
бити проблем квантификовати безбедносно понашање од стране запослених, јер се оно неретко прећуткује од стране запослених. Запослени морају схватити да је њихово ново понашање успешно или да стари начин поступања није успешан.

Повратне информације, награде и казне, играју виталну улогу у процесу промене културе. Претходно су изнете обавезе „топ менаџмента“, али овде је од суштине важности однос средњег менаџмента, будући да он запосленима даје повратне информације, поред тога што такође имају улогу у давању сопственог примера у бебедном понашању. Повратне информације подразумевају и континуирано информисање запослених о безбедносним инцидентима, који су у вези са иницираним променама. Поред тога, повратне информације помажу запосленима да лакше уоче ризик, који је покренуо промене. На основу дефинисаног мерења (квантификације), запослени се могу наградити или казнити, у зависности од њиховог доприноса успешности захтеване промене.

Ревизија представља основни принцип организационе промене. Некада промене које се траже у пракси нису применљиве, а некада их не подржавају запослени. У сваком од случајева управа треба да редефинише првобитно одређени циљ и да размотри његову основаност, односно да утврди нови начин како да га постигне (па тако на пример запослене може да кажњава, или да их „поткупи“).[124]

Полазећи од предмета нашег истраживања, приредили смо Схему организационе промене културе безбедности информација, засноване на едукацији запослених и изведене на основу изнетог у овом раду:[125]

Схема број 4: ***Организациона промена културе безбедности информација засноване на едукацији запослених***



[124] Niekerk, J. F, *op.cit*., стр. 100.
[125] *Ibid*., стр. 101.

xiii. Обликовање перцепције менаџера кроз обуке о развоју безбедносне свести

Овај рад за предмет истраживања има обуке за развој безбедносне свести код менаџера, где аутор разматра који је најбољи приступ у осмишљавању садржаја таквих тренинга.[126]

Аутор примећује да су обуке углавном социо-техничке природе, а да та чињеница и не чуди јер су безбедносне политике често техничке природе, јер се менаџери који се баве пословима заштите информација, претежно ослањају на смернице које су такође технички оријентисане.

Харис је за потребе свог истраживања направио низ видео записа о тренингу о развоју безбедносне свести, и те материјале је поделио у четири групе. У првој групи, били су материјали који су представљали социо-технички аспект безбедности, у другој је био само социјални аспект, трећа је била са техничким аспектом безбедности, а четврта је представљала контролну групу, са садржајем који није повезан са безбедношћу информација. Свакој групи је приказан одређени видео садржај, а потом су утврђене вредности које група има према заштити информација, на основу безбедносних циљева за које су се они определили (реч је о Делфи методу) и том приликом је група са социо-техничким приступом произвела најјачу политику заштите информација, када се погледају циљеви које треба остварити овим видом заштите (дакле циљеви нису једнострани, у смислу да преовладава социјални или технички контекст).

Много теоретичари су већ потврдили да је социо-технички приступ најпогоднији за развој свести о безбедности информација, а аутор у том смислу наводи више извора.[127]

Ипак, новија истраживања (у односу на изворе на које се претодно позива), говоре у прилог томе да постоји недостатак социјалних аспеката. Аутор у раду коментарише овакво стање и образлаже га мишљењем да *корпоративне политике безбедности информација састављају менаџери који имају мало искуства и знања о писању безбедносних политика. Излаз проналазе у томе да се ослањају на политике неке друге организације, као и на комерцијално доступне изворе, као што је интернет. Ту их чекају контролне листе (*чек листе, енгл: *checklists) или стандардизоване смернице, које су технички оријентисане. Харис у том смислу наводи истраживање (Ernst & Young's) из 2008. године, које тврди да је 70% анкетираних организација користило стандардизоване смернице за креирање безбедносних политика, као и да се очекује пораст овог тренда.*[128]

Проблем са чек листама је, наводи аутор, што немају флексибилност за прилагођавање пословном систему у којем се користе. То се посебно одражава на недостатак

[126]Harris. M. A.: *The shaping of managers security objectives through information security awareness training,* dissertation for the degree of Doctor of Philosophy, Virginia Commonwealth University, Richmond, Viginia, USA, 2010.
[127] *Ibid*., стр: 4.
[128] *Ibid*., стр: 6.

социјалним аспектима безбедности. Менаџери којима недостаје знање за стварање социо-техничких политика заштите информација креирају политике засноване на чек листама и неизбежно не успевају да максимизују безбедност информација јер не укључују социјалне аспекте безбедности.

Развијање снажне безбедносне културе, такође је повезано са информационим системима који су безбеднији од других, износи аутор. Култура безбедности одражава вредности и уверења о заштити информација које деле сви чланови неке организације.

Посебан допринос изучавању нашег предмета истраживања, Харис је дао преношењем резултата истраживања односа организационе културе и безбедносе културе, који је радио Руигхавер (енгл: *Ruighaver*) са сарадницима 2007. године.[129] Према том истраживању, они сугеришу да је безбедност информација проблем управљања и безбедносне организационе културе организације, те да одражава на који начин топ менаџмент решава проблеме у организацији. Претпостављајући да на безбедносну културу утиче организациона култура, аутори истражују културу безбедности користећи осмодимензионални оквир за проучавање организационе културе, где су утврдили неколико аспеката добре безбедносне културе, и то: [130]

- организације са висококвалитетном безбедносном културом треба да нагласе дугорочну посвећеност заштити информација;
- потребно је утврдити степен поверења и одговорности запослених према безбедности информација;
- запослени који су одговорни за одређене аспекте безбедности треба да имају снажан осећај власништва над тим аспектима;
- одговорност за доношење одлука о безбедности треба да буде јасно дефинисана у пратећим политикама;
- важна је едукација запослених о њиховим улогама и одговорностима према заштити информација;
- добра безбедносна култура треба да пронађе равнотежу између унутрашњих циљева организације и спољашњег амбијента.

Остале аспекте безбедносне културе, као што су ставови, норме и заједничка очекивања, ови аутори нису уклопили у оквир истраживања, али су их сматрали такође важним, износи Харис.

Једно друго истраживање, које је радио Лич (енгл: *Leach*) разматра шест фактора који имају утицај на безбедносно понашање људи, као и три корака које организације могу да предузму како би помољшали то понашање. Он износи да претње укључују корисничке грешке и немар, као што је заборављање да се примене безбедносне процедуре и злонамерна дела, попут слања осетљивих података без заштите. Фактори

[129] Аутор се позива на извор: Ruighaver, A., Maynard, S., & Chang, S., *Organizational security culture: extending the end-user perspective*. Computers & Security, 26, стр. 56. – 62., 2007. година

[130] Аутор наводи извор: Detert J, Schroeder R, & Mauriel J., *A framework for linking culture and improvement initiatives in organisations*. The Academy of Management Review, 25(4), 2000., 850–63.

који утичу на безбедносно понашање потичу из културе (и праксе) организације, и могу се поделити на две овласти:

- разумевање запосленог шта компанија очеује од њих, у смислу безбедног понашања (оно што им се каже, оно што виде да практикују други и – оно што је њихово искуство из прошлости у погледу њиховог понашања);
- факторе који утичу на спремност запосленог да остане унутар прокламованих норми (лична воља, осећај обавезе према послодавцу, степен потешкоћа које ће имати уколико се не понаша на одговарајући начин).

Овај аутор сматра да се организације могу фокусирати на три кључна фактора како би постигле жељено понашање запослених, у погледу заштите информација. То су понашање од стране менаџмента (давање примера), разум запосленог да прихвати жељени образац понашања и психолошки уговор корисника са својим послодавцем. На крају, Лич изводи закључак да се повезивањем изнетог у његовом истраживању, може закључити да се добро понашање запосленог према заштити информација може постичи следећим:[131]

- обезбедити добро безбедносно понашање свих запослених;
- давати повратне информације о исправности понашања у веи са безбедношћу;
- давати награде запосленима за безбедно понашање;
- пружити додатну обуку запосленима који показују лоше безбедносно понашање;
- научити запослене безбедносним принципима који ће им омогућити доношење добрих одлука у заштити информација;
- створити снажну безбедносну културу и мотивисати запослене да се понашају доследно;
- редовно разговарати са запосленима о безбедности (и са управом и са запосленима).

Истраживање је показало да природа и опсег обуке за заштиту информација која се даје менаџерима утиче на природу и обим политика о заштити информација. Тренинг појачава њихов начин размишљања о безбедности, а самим тим и политике безбедности информација које се креирају – што у крајњем доводи до модификације будућих обука о информационој безбедности.

Полазећи од предмета нашег истраживања, напомињемо да смо читајући овај рад пронашли и охрабрење за наше ставове, будући да се Харис осврнуо на рад Дилана, где је у разматрању дефинисања информационог систем изнето да се он састоји од три нивоа: техничког, формалног и неформалног, о чему смо коментарисали детаљније у идејном пројекту нашег рада и где смо дали нашу схему на основу ових ставова (Схема број 1: *Нивои информационог система према Дилану*).

[131] Mark A. Harris, *op.cit.*, стр. 20. – 21.

xiv. Закључна разматрања поглавља

За претрагу релевантин научних радова, који су у вези са нашим предметом истраживања: заштита информација у банкама и финансијским институцијама, првенствено полазећи од организационог и нормативног аспекта уређења и обављања ових послова, користили смо интернет претрагу објављених научних радова, и то КоБСОН[132], *Sciencedirect*[133], односно друге слободне интернет претраживаче, у складу са наведеним у одговарајућим напоменама.

У хипотетичком оквиру навели смо да се заштита информација у банкама и финансијским институцијама у пракси базира на информационој (*IT*) безбедности, чиме се имплицира развој других неопходних аспеката овог система заштите, а посебно у организационом и нормативном смислу.

Такође, радови које смо ми изучили управо говоре о томе да се *информациона безбедност не може посматрати (само) са техничког аспекта*, већ је исправан приступ да се у обзир узму и други аспекти које аутори различито називају, али се њихова идеја своди на потребу разматрања нетехничких мера, које обухватају нормативне и организационе аспекте.

Алнатир[134] је тако утврдио да се *сигурност информација бави људима, процесима и технологијом*, а многи други аутори чије смо налазе приказали у овом поглављу се слажу да су људи у том ланцу најслабија карика. Тако је овај аутор пронашао да се у вези са безбедносном културом у организацијама, издвајају следеће проблемске области које истраживачи третирају:

- подршка менаџмента информационој безбедности;
- политике и спровођење информационе безбедности;
- свест о информационој безбедности;
- тренинг о информационој безбедности;
- процена ризика у информационој безбедности;
- контрола усклађености у информационој безбедности;
- организациона култура;
- правила понашања.

Све наведене области, наша је примедба, управо се могу класификовати у нормативне и организационе мере у остваривању заштите информација.

---

[132] Доспутно на: https://kobson.nb.rs/%D0%BA%D0%BE%D0%B1%D1%81%D0%BE%D0%BD.749.html#.XoODB0Azbcs

[133] Доступно на: https://www.sciencedirect.com/

[134] Alnatheer, S. M. A.: *Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia,* PhD Thesis, Faculty of Science and Technology, Queensland University of Technology, Brisbane, Queensland, Australia, 2012.

Алфаваз, слично томе, тврди да поред улоге технологије (пренесено на смисао нашег истраживања – поред IT безбедности) кључну улугу у *култури информационе безбедности* има улуга менаџмента. Они заједно са запосленима утичу на вредности које су некада видљиве а некада не. Те вредности, заједно са активностима које здружено пружају технологија и активности менаџмента стварају праксу која може бити различита у погледу статуса знања и активности запослених. У том смислу аутор разликује четири мода у којима може бити организација, у којем је прихватљиво само када у организацији има и знања (о безбедности информација) и када постоје одговарајуће активности.[135]

Коскокас[136], прави *друштвено−организациони приступ* у управљању безбедности информационих система у конктексту интернет банкарства, а свој приступ заснива на претпоставци да се безбедност информационих система може посматрати само кроз системско и свеобухватно проучавање различитих аспеката друштвене организације (технички аспект се том приликом не доводи у питање). Он напомиње да дотадашња пракса (успостављања система безбедноси информација у интернет банкарству) препознаје четири раличите фазе и то: Прве две генерације имају за циљ да открију шта се може учинити у отклањању претњи, па с тога доминирају принципи, чек листе и већина безбедносних стандарда за развој система. Трећа генерација укључује моделирање, а четврта наглашава управо социотехнички дизајн. Коскокас наводи да су концепти поверења, културе и комуникације блиски и међусобно повезани, али и да нису увек међусобно зависно променљиве. То значи да ови аспекти могу постојати унутар организације независни један од другог. Као пример он наводи да, култура у организацији може бити јака, али ниво поверења низак, иако јесте утврђено да поверење олакшава успостављање снажне културе унутар организација и ефикасност комуникације коју треба постићи.

Организационе промене, имају значајну улогу за остваривање заштите информација. Биркланд,[137] говори о неминовности у промени концепта безбедности, који доноси модерно банкарство. Захваљујући интернет банкарству, безбедност постаје друштвени проблем, у којем се јављају и нове методе угрожавања (као што је *phishing*). Одатле ће се, тврди аутор, банке у будућности бавити следећом групом питања.

- потрагом за дефиницијом савремене банке;
- питањем одговорности менаџмента (лидера);
- питањем одговорности запослених;
- како дефинисати безбедност у контексту „новог банкарства“;
- која ће бити стратегија безбедности корисника.

[135] Alfawaz, S. M.: *Information security management: A case study of information security culture*, Faculty of Science and Technology, Queensland University of Technology, 2011., стр. 226. – 233.
[136] Koskosas, I., V.: *A Socio-Organizational Approach to Information Systems Security Management in the Context of Internet Banking*, A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing at St. John's Brunel University, London, UK, 2004.
[137] Birkeland, S.: *E-Banking security and organisational changes*, PhD, University of Liverpool, 2015.

Можда је за поставку његових питања о информационој безбедности у банкама најпригоднији пример који је сам дао. Он каже да је Тесла (произвођач аутомобила) много више IT компанија, него што припада традиционалној ауто индустрији, и ако је главни производ аутомобил. Тесла приоритетно има потребу за сигурношћу, ажурирањем софтвера аутомобила на мрежи, и иначе све се обавља путем онлајн решења. На исти начин банке управљају новцем људи или компанија, којом приликом је већина контаката са купцима на мрежи.

Нормативни оквир, од значаја је за функцинисање заштите информација у банкама, јер он утиче на свест о безбедности корисника (енгл: *security awareness*). Наше је мишљење да се под корисницима могу посматрати не само клијенти банке, већ да су то и сами запослени (јер и они користе информатичке ресурсе и на тај начин учествују у заштити информација). Такође, ово је још једно место у нашем истраживању где видимо да се нормативни и организациони аспекти у остваривању заштите информација сусрећу и прожимају, јер нормативне норме саме по себи не представљају само скуп закона и подзаконских аката, како у литератури често наводе – *безбедносне политике*, већ се њихова примена највише огледа у свести о безбедности, која је фундаментална за организацију и њену културу. Либота у свом раду наводи примере најбоље праксе у погледу заштите информација, да би на крају извршила анализу празнина које се јављају када се упореде најбоља пракса и законске обавезе банака.[138]

Да научна гледишта у погледу значаја нормативног и организационог приступа у остваривању заштите информација нису сасвим усаглашена, што смо уосталом и ми изнели кроз искуствено опажање праксе која нас окружује, пронашли смо у раду Калида и Али Курешија.[139]Они у свом раду пореде праксе у управљању IT безбедности (дакле не управљању информационом безбедности), у различитим културама: Шведској и у Пакистану. Насупрот нашим очекивањим да ће у истраживању као зависне варијабле бити посматрани организациони аспекти, у ширем контексту (односи националне културе, организационие културе, културе безбедности ифнормација), они се фокусирају само на техничке аспекте информационе безбедности. Из тих разлога они дају вулгарни приступ, наше је мишљење, где виде као основни елемент управљања сигурношћу информација Политику IT безбедности, која представља основни документ из којег извиру процедуре и подполитике (што није спорно).

Путник наводи да несигурност кибер простора има двојаку основу, и то су:[140]

---

[138] Lee Botha, C.: *A Gap Analysis to Compare Best Practice Recommendations and Legal Requirements when raising Information Security Awareness amongst Home Users of Online Banking,* Submitted in accordance with the requirements for the degree of Master of Science in the subject Information Systems, University of South Africa, 2011.

[139] Khalid, F., Qureshi, M.: *How companies manage IT security A comparative study of Pakistan and Sweden*, master thesis in informatics, Jönköping International Business School, Jönköping University, Sweden, 2013.

[140] Пунтик, Н.: *Кибер ратовање – нови облик савремених друштвених конфликата,* докторски рад, Факултет безбедности, Универзитет у Београду, Београд, Република Србија, 2012. година

- технички разлози;
- грешке и пропусти организације и индивидуалних корисника приликом коришћења („људски фактор“).

Грешке које чине људи посебно привлачи нашу пажњу, јер како он наводи, неретко образовања корисника о безбедности сопствених система није адекватно. Ми смо у досадашњем прегледу научне литературе, као и искуственим опажањем, ово становиште сусретали код проблема подизања нивоа свести код корисника (енгл: *security awareness*), који са аспекта банкарског пословања могу бити и клијенти, али и сами запослени банке.

Уосталом, Путник наводи да је *недостатак безбедносне културе* уочљив и на индивидуалном и на нивоу предузећа и организација, што је у сагласности и са нашим хипотетичким оквиром. Аутор наводи да вртоглаву експанзију Интернета не прати и одговарајућа специјализација стручњака на пољу информационе безбедности, па тако цитира Е. Спафорда (E. Spafford), директора Центра за едукацију и истраживање у области информационог осигурања и безбедности универзитета Пардју (енгл: *Purdue University, Public university in West Lafayette, Indiana, USA*): „Безбедност није могуће лако додати накнадно, што знатно отежава задатак професионалцима безбедносног сектора. Софтвер и хардвер који се данас користе пројектовани су неправилним методима, а такође се накнадно лоше тестирају, од стране особа које знају мало или готово ништа о безбедности, што је резултовало непоузданим резултатима. Затим се додају постојећој инфраструктури, која је већ пуна слабости и којом управља, и користи је, особље недовољно упознато са ризицима. Нико не би требало да се изненади повећањем броја напада и вируса у годинама које следе.“.[141]

Путник је у свом раду дао класификацију субјеката претњи у кибер простору, где смо ми препознали области где треба тражити упориште за изгрању система безбедности информација, односно одакле се назире простор који је потребно попунити да би та заштита била адекватна, као и где се може остварити увид колико је погрешан приступ да se заштита информација може остварити само техничким знањима и без знања о безбедности, врло користан и инспиративан за даља разматрања.[142]

У раду је приказан преглед перцепције самих запослених, према истраживањуо томе са које стране долази претња за безбедност информационг система, према којем је структура претњи таква да око 80% претњи долази од стране хакера и *од стране самих запослених*[143].

Мотивисаност инсајдера за нарушавање безбедности, како наводи аутор, може бити различита и да потиче од:

- другачијег система вредности у односу на организацију која их запошљава;

[141] *Ibid*., стр. 83. – 87.
[142] *Ibid*., стр. 203
[143] 2003 CSI/FBI Computer Crime and Security Survey, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

– радозналости, освете, уцене, изнуде, мотива нелегалне зарада и др.

Једна од могућих стратегија за ублажавање овог ризика је стално *информисање запослених о ризицима, организационој политици и безбедносним процедурама*. Такође, корисна тежња би била и запошљавање поузданог и поверљивог особља, одакле опет, са становишта нашег предмета истраживања, видимо на примеру колико је *важна сарадња више пословних функција у организацији* (у овом примеру *HR*-а и безбедносне пословне функције) у остваривању заштите информација. [144]

Посебан значаја за предмет нашег истраживања, Путник је дао кроз одређивање *Модела вишеслојне заштите*, према којем претња, да би била реализована, треба да прође више прстенова заштите, и то:[145]

– физичку заштиту;
– техничку заштиту;
– кадровску заштиту;
– организациону заштиту;
– нормативну (регулаторну) заштиту.

Организиациона заштита подразумева организациону структуру, дефинисање радног процеса, развој софтверских система, праћење смерница и стандарда, планирање и друго. Подразумева и праћење међународних и националних безбедносних стандарда у овој области.

Нормативна заштита, подразумева законе, упутства, планове и другу регулативу која обевезује и прописује извршење неке радње и начин извршења те радње
Станаревић је у свом раду извршила анализу теоријских поставки појмова културе и *безбедносне културе*.[146] Она је кроз призму културе, националне културе, националног идентитета, концепта безбедности и националне безбедности одсликала својства безбедносне културе као специфичне безбедносне инфраструктуре.

Посебну вредност према предмету нашег истраживања смо пронашли у разматрањима о појму безбедности, будући да је реч о појму који се у теорији различито дефинише. Станаревић наводи да су бројне дефиниције и тумачења безбедности, те да је тешко определити се која је у том смислу најпрецизнија. Разлог за овакве околности су различити приступи и критеријуми којима су се аутори водили да би објаснили шта безбедност значи.

Контект *организационе културе* Станаревић је у раду означила кроз одређење Едгара Шајна (*Edgar Schein*), најпознатијиg теоретичара који се бавио организационом културом. Он је дефинисао појам организационе културе као образац заједничких основних претпоставки на основу којих је група научила како да решава проблеме

[144] *Ibid*., str. 272. – 290.
[145] *Ibid*., str. 362.
[146] Станаревић, С.: *Концепт безбедносне културе и претпоставке његовог развоја,* докторски рад, Факултет безбедности, Универзитет у Београду, Београд, Србија, 2012. година

спољне адаптације и унутрашње интеграције, а формулисане су довољно добро да се могу сматрати вредним и као такве преносити новим члановима организације, као исправан начин перцепције, размишљања и осећања за исте проблеме.[147]

Свака организација има јединствену културу, која утиче на брзину промена/иновација. Да би се иновација усталила, неопходно је да је подстичу и прихватају сви запослени и на свим нивоима. Промена се неће укоренити уколико је не прихвати пословодство, или уколико управа не верује у њену вредност, што је нарочито специфично у традиционалним хијерархијским организацијама, наводи Станаревић.[148]

Посебан допринос овог рада је дискусија о контексту културе заштите на раду, односно о контексту културе безбедности и здравља на раду (како слови и Закон који регулише ову област код нас). Наиме, у иностраној теорији и пракси, термини на енглеском језику: *safety* и *security* у доброј мери су дефинисани својим обимом појмовног одређења, тако да се под *safety* подразумевају заштита на раду (некада је ту и против пожарна заштита, а некада она представља посебан појам), а под *security* – безбедност (физичко-техничко обезбеђење, техничка заштита, интерне истраге и друго). Ауторка наводи да организације без обзира на врсту делатности на коју су усмерене, морају обезбедити да ове две културе егзистирају једна поред друге.

Разматрање односа структуре организације (где је мерено учествовање у одлучивању и стандардизацији рада) и свести о безбедности информација; односа између организационе културе (мерено је организационо лидерство и стил управљања) и свести о безбедности информација; односа између политика *HR*-а (мерено је опис послова, провера кандидата, услови запослења, менаџмент одговорности, безбедносна обука) и свести о безбедности информација, пронашли смо у раду који се бави испитивањем односа између организационог система и безбедности информација у десет комерцијалних банака на Тајланду.[149]

Незасвисне променљиве у овом раду биле су централизација, формализација, хијерархија, тржишна култура, и правила и политике Људских ресурса – *HR*-а (енглески: *Human resource policies and practices – HRPP*). Зависна варијабла била је Свест о безбедности информација - ИСА (енгл: *Information Security Awareness – ISA*) корисника.

Аутор је закључио да:

- потребно је повећати учешће запослених у одлучивању, да би се повећала безбедносна свест запослених;
- неуспех планираних промена у организацији (повећање безбедносне културе) последица је занемаривања организационе културе. Подизање свести о

[147] *Ibid*., стр. 243. - 244.
[148] *Ibid*., стр. 246.
[149] Tintamusik, Y.: *Examining the Relationship between Organization Systems and Information Security*, Faculty of the School of Business and Technology Management, Northcentral University, Arizona, USA, 2010.

информационој безбедности (енгл: *ISA*) могуће је организовати управо преко организационе културе, као механизма контроле. Када у организацији постоји безбедносна култура, аспекти информационе безбедности се реализују као природан, рутински и свакодневни приступ од стране запослених;
- информациона безбедност се не може затварати у технички аспект и специфична *IT* знања, већ је потребно да има активну сарадњу са другим пословним функцијама, а пре свега са другим сегментима безбедности

У банкарској индустрији често се расправља о *кризном менаџменту*. Банке теже ка стабилности и сигурности пословања, а кризе представљају све супротно − управо нестабилности и несигурности, један је од налаза у раду који истражује како банке поступају у случају безбедносних инцидената.[150]

Више није питање како, већ када и зашто се јавља криза, пре питања у којем ће се облику она појавити и колико ће организација бити спремна за њено наступање. Интегрално обележје данашњег информационог доба јесте да се криза више не може видети као ретка и случајна појава, већ се она јавља у све већој учесталости.

Аутори износе различита теоријска тумачења концепта кризе, где између осталог наводе да је организациона криза догађај мале вероватноће који има висок утицај који прети одрживости организације и догађај где се мора поступати брзо. Исто тако, наводе и да уколико целокупни процес стратешког планирања не укључује управљање кризама је исто као одржавање живота без гарантовања живота.

Организације, слично као и појединци, постављају *одбрамбене механизме* како би онемогућили и негирали своју рањивост. Тако је Митроф препознао различите врсте одбрамбених механизма који могу постојати у култури организације (и који су блиски са Фројдовом теоријом одбрамбених механизама):[151]

- порицање (криза се дешава другима, наша организација је нерањива);
- омаложавање (кризе се догађају, али ако и погоди нашу организацију, утицај ће бити мали);
- идеализација (криза не погађа добре организације, као што је наша);
- величање (наша организација је тако велика, па ћемо бити заштићени од кризе);
- пројекција (ако се и догоди криза, то је зато што је неко то желео да се догоди)
- интелектуализација (вероватноћа да се догоди је мала);
- парцијализација (ако се догоди криза, не може да утиче на целу организацију).

Израда *безбедносе стратегије за информациону безбедност* у компанијама, предмет је рада Солмса и Солмса, где они наводе да изостављање било којег од аспеката који су навели има за последицу неконзистентност у спровођењу заштите информација у

[150] Andersson, D., Gustavsson, M., Waldén, A.: *How a bank organization handles robberies – a question of crisis management,* Jonkoping International Business scool, Jonkoping University, Sweden, 2008.
[151] *Ibid*.

организацији.[152] Аутори наводе да су то следећи постулати који се не смеју занематири, како они кажу *„десет смртних грехова“*:

1. Информациона безбедност је одговорност највиших управљачких структура
2. Информациона безбедност је приоритетно пословно а не технико питање у организацији
3. Информациона безбедност захтева мултидисциплинарни приступ
4. План информационе безбедности мора се заснивати на утврђеним ризицима
5. У информационој безбедности је потребно примењивати искуства најбоље праксе
6. Безбедносна Политика заштите информација је неоходна (мисли се на кровни документ)
7. Спровођење и надгледање безбедносне праксе у заштити информација је неопходно у организацији
8. Управљање пословима безбедности информација је неопходно у организацији
9. Информисање о безбедности информација је неопходно у организацији
10. Не давање подршке информационој безбедности потребном инфраструктуром и алатима

Ми смо за потребе нашег рада посебно истакли налаз о *неопходности мултидисциплинарног приступа информационој безбедности*, што извире из изнетог у њиховом раду о фокусу на пословно а не техничко питање, када је у питању заштита информација. Безбедност информација је вишедимензионална дисциплина и све димензије се морају узети у обзир да би се осигурало безбедно окружење за информатичке ресурсе компаније. Аутори се позивају на објављену литературу, али и на обављене разговоре са руководиоцима информационе безбедности. Они износе став да листа, како су је дали у овом раду, није коначна, као и да се неке димензије могу преклапати у погледу њиховог саржаја. Коначно, важна је идеја о мултидисциплинарности, а не број и садржај димензија, које су дате према следећем:

- димензија политике;
- димензија најбоље праксе;
- етичка димензија;
- димензија цертификације;
- правна димензија;
- димензија осигурања;
- особље / људска димензија;
- димензија свести;
- техничка димензија;

[152] *The 10 deadly sins of information security management,* Basie von Solms, Standard Bank Academy for Information Technology, Rand Afrikaans University, Johannesburg, South Africa; Rossouw von Solms, Faculty for Computer Studies, PE Technikon, Port Elizabeth, South Africa, Computers & Security (2004) 23, 371. – 376., 2004.

- мерење / метрике (надгледање усклађености / *IT* ревизија у стварном времену);
- димензија ревизије.

Уочљиво је, истичу аутори, да је *већина димензија нетехничке природе*, и да се оне морају све узети у обзир приликом израде свеобухватног плана информационе безбедности предузећа. Последица овог греха је стално враћање на процес планирања, јер ће се у пракси увек јавити недоследности и нелогичности.

Провејава кроз многе радове које смо анализирали, а често се то и експлицитно наводи, да је *едукација корисника за заштиту информација* један од кључних фактора у остваривању заштите информација. Обичпно се говори о развоју безбедносне свести (енгл: *Security Awareness*). Никерк у свом раду о успостављању организационе културе информационе безбедности на основу едукације корисника, полази од стандарда ISO 17799, који даје препоруке најбоље праксе за покретање, примену или одржавање система управљања сигурношћу информација.[153] Једна од кључних активности јесте увођење програма о безбедносној свести у заштити информација, где је суштина у едукацији корисника о појединачним улогама које они имају у остваривању овог система.

Развој безбедносне свести представља круцијални елемент заштите, па се даље поставља питање на који начин приступити овој активности у организацији. Никерк у свом раду износи становиште, засновано на дотадашњим теоријским истраживањима, да је добра околност да постоје стандарди и смернице које упућују организацију на потребу организовања обуке за информациону безбедност, али исто тако и да су оне начелне и да не дају одговор на питање шта је то одговарајућа обука. Аутор наводи да *стандарди занемарују одговарајуће образовне принципе, што се усложњава чињеницом да програме за развој безбедносне свести формирају углавном IT професионалци, који (*осим техничких, наша је примедба*) немају потребна знања која су потребна да би се организовали програми обуке овако важне и комплексне области, као што је заштита информација* (образовни принципи, контекст безбедности у пословном окружењу, садржај безбедности као појма и као пословне функције и друго, наша је примедба).

С тим у вези, аутор износи став да би у образовању одговарао приступ који сваки део образовног система заснива на циљевима (енгл: *outcomes-based education − OBE*).[154]Овај приступ у ствари може бити идеалан за употребу у програмима, с

---

[153] Niekerk, J. F.: *Establishing and information security culture in organizations: an outcomes based education approach*, Dissertation submitted in fulfillment of the requirements for the degree Magister Technologiae in Information Technology, Faculty of Engineering, Nelson Mandela Metropolitan University, University in Port Elizabeth, South Africa, 2005.

[154] ОБЕ је теорија образовања која сваки део образовног система заснива на циљевима (исходима). На крају образовног искуства, сваки је ученик требао постићи циљ. У ОБЕ нема одређеног одређеног стила предавања или оцењивања; Уместо тога, часови, прилике и оцене треба да помогну ученицима да постигну задане исходе.

обзиром да циљ није припремити полазника за испит или за даљи ниво формалног образовања, већ управо има функцију да помогне полазницима да постигну конкретан циљ, у нашем случају – свест о информационој безбедности.

Никерк наводи у свом раду да у теорији нема знања о погодности ОБЕ-а за креирање корпоративних образовних програма у информационој безбедности. Он је овај проблем видео као двострук, и то:

- безбедност информација зависи од људи који су укључени у процес заштите информација, а тренутни програми не придају довољно пажње теоријама понашања. Едукација заснована на резултатима је педагошка методологија која би могла бити погодна за стварање информационе сигурности
- неговање организационе субкултуре безбедности информација је неопходно у организацији. У теорији је добро проучен проблем промене корпоративне културе, али је недовољно проучен процес промене субкултуре заштите информација.

Начелно, организације треба да прилагоде своје програме за развој свести о безбедности на такав начин да уваже своје конкретне потребе и структуру запослених (профил радне снаге, опис њихових послова, интерну организацију рада, старосну и образовну структуру, њихово радно искуство и друго). Како се у организацијама по правилу ради о одраслој популацији, потребно је уважити и педагошка правила која важе за образовање одраслих.

Аутор је предложио критеријуме које би овакви програми требало да испуњавају, и то:

- сви полазници треба да буду у прилици да „прођу“ тренинг;
- запослени треба да разумеју због чега су им потрене вештине које уче, односно због чега треба да се понашају на одређени начин;
- материјале за учење треба прилагодити стилу учења;
- полазници треба да су одговорно за своје учење;
- полазници треба да добију повратне информације о успешности обуке.

Теорија организационог учења, наводи аутор, није сама по себи довољна за промену корпоративне културе организација, већ је потребан формализовани процес управљања променама који долази из менаџерских наука. Било који покушај промене заједничких прећутних претпоставки, уколико није спроведен на одговарајући начин, могао би да резултира психолошком анксиозношћу међу запосленима.

Ми смо на основу изнетог у раду Никерка дали Схему организационе промене културе безбедности информација, засноване на едукацији запослених.

Важност безбедносних обука у информационој безбедности дао је Харис, проучавајући перцепцију менаџера која се ствара кроз ову активност.[155]

Аутор примећује да су обуке углавном техничке природе, а да та чињеница и не чуди јер су безбедносне политике често исте природе, јер се менаџери који се баве пословима заштите информација, претежно ослањају на смернице које су такође технички оријентисане (мисли се на стандарде, чек листе и друго, наша је примедба). Аутор наводи да новија истраживања говоре у прилог томе да постоји недостатак социјалних аспеката. *Корпоративне политике безбедности информација састављају менаџери који имају мало искуства и знања о писању безбедносних политика. Излаз проналазе у томе да се ослањају на политике неке друге организације, као и на комерцијално доступне изворе, као што је интернет. Ту их чекају контролне листе (*чек листе, енгл: *checklists) или стандардизоване смернице, које су технички оријентисане. Харис у том смислу наводи истраживање (Ernst & Young's) из 2008. године, које тврди да је 70% анкетираних организација користило стандардизоване смернице за креирање безбедносних политика, као и да се очекује пораст овог тренда*[156]

Проблем са чек листама је, наводи аутор, што немају флексибилност за прилагођавање пословном систему у којем се користе. То се посебно одражава на недостатак социјалним аспектима безбедности. Менаџери којима недостаје знање за стварање социо-техничких политика заштите информација креирају политике засноване на чек листама и неизбежно не успевају да максимизују безбедност информација јер не укључују социјалне аспекте безбедности.

У дефинисању нашег идејног пројекта истраживања, на основу изнетог у овом Харисовом раду где се позивао на Дилана, дали смо Схему нивоа информационих система где је у разматрању дефинисања информационог систем изнето да се он састоји од три аспекта: техничког, формалног и неформалног.[157] Формални и неформални ниво, како смо дали према Дилану, одговара управо организационим и нормативним аспектима заштите информација.

Налази добијени прегледом научних радова који се односе на наш предмет истраживања, дали су нам добре претпоставке за даље истраживање заштите информација у организационом и нормативном аспекту објашњења овог феномена, и поред чињенице да научни допринос у предметној области до сада није био издашан. У даљем раду, ми ћемо се фокусирати на рашчлањивање нашег предмета истраживања, како је то, видели смо из претходно наведеног у овом поглављу, дала досадашња научна литература, па ће посебно бити наглашени појмови заштите

[155] Harris, M. A.: *The shaping of managers security objectives through information security awareness training,* dissertation for the degree of Doctor of Philosophy, Virginia Commonwealth University, Richmond, Viginia, USA, 2010.

[156] *Ibid*., стр: 6.
[157] *Ibid*., стр: 9.

информација, организационе културе, пословних функција у банкама чија конвергенција чини систем безбедности, и друго.

II ИНФОРМАЦИОНА БЕЗБЕДНОСТ

1. Значај заштите информација

Област заштите информација данас је једнако раширен појам у свакодневном животу, као што су и други информатички ресурси и тековине које савремени човек користи у приватне и пословне сврхе.

Готово да нема области живота где информатичка револуција није довела до промена у начину комуницирања и обављању свакодневних послова. Из тих разлога, заштита информација је природно постала тема којој пажњу посвећују готово сви. Овим проблемом баве се људи на нивоу појединца, микро, малих и средњих предузећа, па све до великих корпорација, држава и међудржавних заједница.

Банке и финансијке институције нису изузетак, а њихово интересовање за заштиту информација и информатичих ресурса извире из осетљивости које они имају за пословање и имовину ових правних субјеката. Штете које банке могу да претрпе, када су угрожене ове виталне вредности крећу се од оних подношљивих па до катастрофалних штета због којих у питање може да дође и само даље пословање. Поред ових директних штета, информациони инциденти могу да доведу и до других, нематеријалних штета, о чему ће касније бити више речи о нашем раду. Услед значаја које банке и друге финансијске институције имају за економију, о безбедности у том смислу воде рачуна и државе и државне заједнице.

Наука није остала имуна на значај који данас има информатичка сфера живота, па се о заштити информација говори и дискутује и у овој области друштвеног битисања. Без научних достигнућа и истраживања, ни област заштите информација не би могла да напредује и да води трку са изворима угрожавања и различитим облицима претњи.

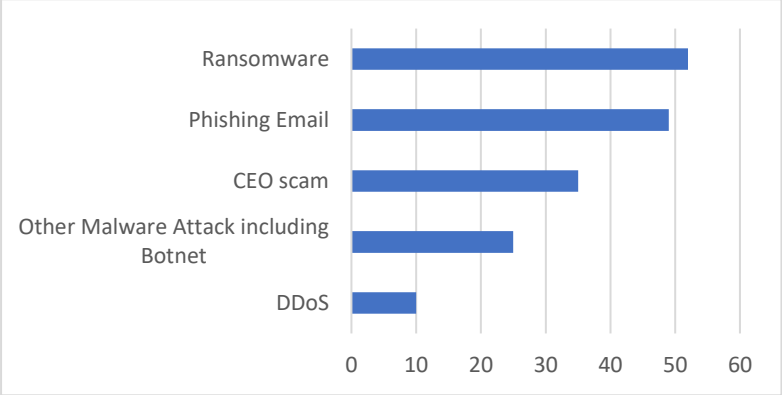
На међународној конференцији о интернет технологијама, одржаној пре годину дана у Хонг Конгу, на отварању конференције уводничар је у својој презентацији изнео чињенице о изазовим и достигнућима који се односе на сајбер безбедност.[158]

[158] Hui, K. L.: *Cybersecurity: Challenges and Recent Developments,* Department of Information Systems, Business Statistics and Operations Management (ISOM), Hong Kong University of Science and Technology (HKUST), Hong Kong, 9th International Conference on Internet Technologies & Society, 2019.; доступно на:

Полазећи од предмета истраживања нашег рада, и као увод у поглавље у којем ћемо се осврнути на основне појмове информационе безбедности, изнећемо неколико чињеница које најбоље описују значај који има овај вид заштите за пословање у данашњем свету.

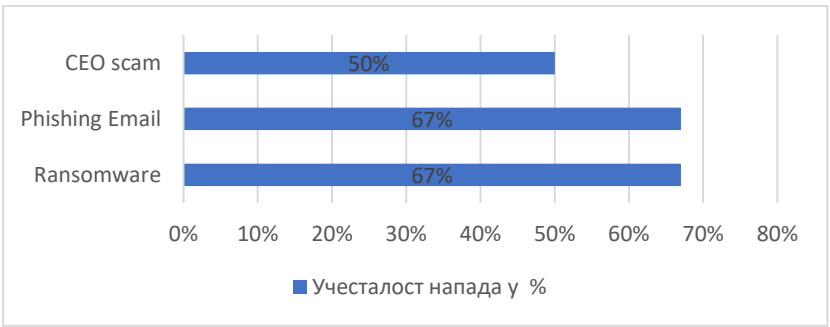
Лунг Хуи, је тако изнео податак да су у току 2018. године, најчешће јављале следеће врсте сајбер напада:[159]

Графикон број 1: ***Најучесталији сајбер напади у 2018. години***



На конференцији је изнет податак о учесталости ових напада према врстама индустије где су се догодили, а *када су у питању банке и финансијске институције, сајбер напади су се догодили према следећој учесталости*: CEO scam, Phishing Email i Ransomware напади. Не улазећи сада у детаљнија објашњења, навешћемо да је реч о претњама које су у својој основи комбинација претњи које долазе из техничке и друштвене сфере (јер се односе на понашање људи). Што је од значаја за наш предмет истраживања, будући да је ово аргумент да ни мере заштите не могу онда потицати само из једне сфере, већ оне морају да укључе и техничке и нетехничке мере заштите.

Графикон број 2: ***Највеће претње за финансијске институције у 2018. години***



http://its-conf.org/oldconferences/2019/wp-content/uploads/2019/02/ITS-2019-Keynote-Speech-on-Cybersecurity.pdf

[159] *Ibid*

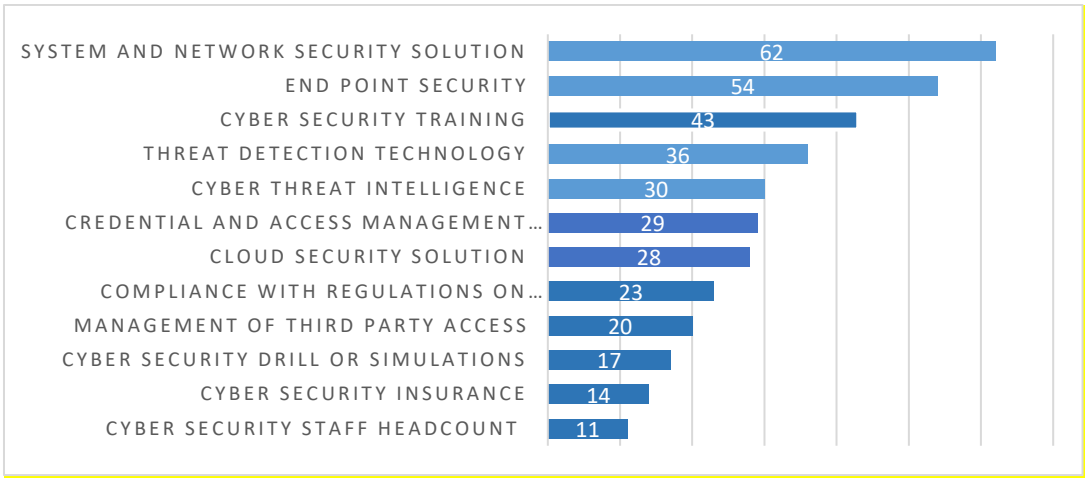
Следствено наведеном, банке и финансијске институције предузеле су следеће мере и активности:

Табела број 2: ***Спремност финансијских институција за сајбер напад у 2018. години***

ОБЛАСТ ЗАШТИТЕ	0 – 100%
Процена ризика/ Security Risk Assessment	64,8%
Техничке контроле/Cyber Threats Detection	52,8%
Процесне контроле (привилегије, data backup, Third party risk management)/Process Control	71,2%
Обуке особља за заштиту информација/Security Awareness	53,3%

Области информационе безбедности у које су организације највише улагале су дате према следећем:

Графикон број 3: ***Области информационе безбеднсоти према улагањима компанија у 2018. години***

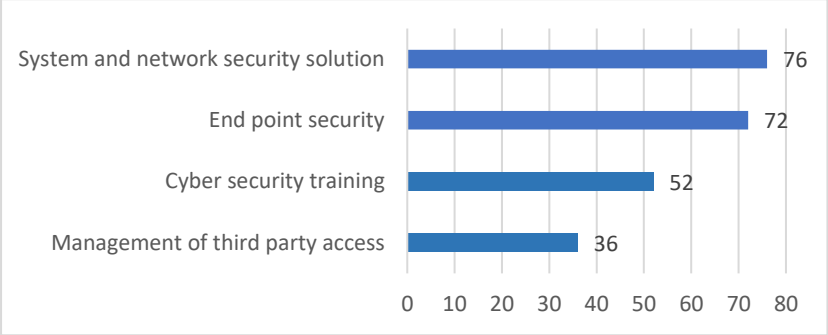


Полазећи од предмета нашег истраживања, ми смо у графикону обележели тамнијом бојом оне *мере које су нетехничке природе*. Ми ћемо касније у раду више говорити о овим мерама, а на овом месту ћем навести да је реч о следећим нетехничким мерама:

- тренинзи за повећање безбедносне свести запослених у заштити информација;
- усаглашеност организација са нормативом из области сајбер безбедности и заштите личних података о личности;
- *management of third party access*;
- извођење вежби и симулација за сајбер нападе;
- улагање у полисе осигурања за случај сајбер напада;
- улагање у специјализовано особље за одбрану од сајбер напада.

Банке и финансијске институције највише су улагале у следеће области заштите информација (Графикон број 4: *Области информационе безбедности према улагањима финансијских институција у 2018. години*):

Графикон број 4: Области информационе безбедности према улагањима финансијских институција у 2018. години



Из прегледа видимо да су банке и финансијске институције једнако улагале у техничке и нетехничке мере заштите, као и да су у том смислу најзаступљенији: тренинзи за повећање безбедносне свести запослених у области заштите информација и *Management of third party access.*[160]

Ову широку слику амбијента у којем данас функционише заштита информација у сектору банкарства и других финансијских институција, дали смо као прилог изнетим тврдњама о значају наше проблемске области и уместо увода у поглавље у којем имамо намеру да размотримо основна разматрања о заштити информација.

[160] Истраживање из 2018. године о приступу мрежи организација од стране пословних сарадника који имају такву потребу (одржавање мреже, ажурирање софтвера и сл.), наводи да се је на основу анкете, у којој је учествовало више од хиљаду стручњака за заштиту информација, утврђено да 94% организација дозвољава корисницима трећих страна приступ њиховој мрежи, а да 61% испитаника нису сигурни да ли су ови приступали датотекама или подацима за које нису овлашћени. Запослени код „трећих страна“, имају привилеговани приступ у 72% случајева, а само 22% испитаника тврди да зна да њихови трећи корисници не покушавају неовлашћени приступ информацијама, док је 18% анкетираних потврдило да су запослени треће стране успешно приступили информацијама за које нису овлашћени. Само 21% испитаника је изјавило да одмах блокира или укида приступ трећим корисницима када њихово ангажовање престане. Такође, само 15% анкетираних је изјавило да су уверени да њихове треће стране поштују правила приступа (чување корисничких имена и лозинки − *креденцијала*), док 25% сумња да треће стране поштују правила управљања приступом, али су убеђени да то не чине. Чак 45% испитаника је дало исказ да трећој страни верује више него сопственим запосленима, у погледу поштовања безбедносних смерница. У 20% финансијских организација су признали да је трећа страна приступила или је покушала да приступи датотекама или подацима за које нису овлашћени. Доступно на: https://betanews.com/2019/11/20/third-party-access-organizations-exposed/

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

Прегледом литаратуре, као и искуствено, запазили смо да се појмови „cyber“, или „кибер безбедност“ често поистовећују са појмом „безбедност информација“, „информациона безбедност“ и слично.

Овај однос обима појмова није безначајн, будући да сматрамо да он имплицира приступ који теоретичари, као и практичари, могу имати у настојању разумевању њиховог поља истраживања, односно рада.

У истраживању о овој теми, наводи се да питање није безбачајно, јер многа банкарска регулаторна тела (наводи се као пример Банка Индије и монетарне управе Хонг Конга и Сингапура) захтевају од банака да имају одвојене политике безбедности информација и сајбер безбедности.[161]

Да ли је реч о синонимима или не, али знамо да они сигурно стварају забуну међу стручњацима безбедности, наводи се у раду. Ми смо такође искуствено запазили, да се у разговору са домаћим стручњацима, могу срести оба приступа. Индикативно је да они обично мисле, у зависности од личног става, да један термин подразумева и други, у било којем приступу.

Полазећи од проблема нашег истраживања, ми нећемо детаљније разматрати овај однос обима појмова, али ћемо означити да он постоји и да будућа истраживања треба да се посвете и овом питању.

Наша је претпоставка да терминолошку неуређеност, о којој је реч, треба посматрати из перспективе значења појмова, у погледу разлика између термина „податак“ и „информација“, што је наука већ решила као проблем. У тексту се наводи да је, на пример, број 14.02.1960. податак. Ако се овај податак интерпретира у контексту, на пример да знамо да је ово датум рођења неке особе, онда имамо информацију. Слична поређења смо пронашли и ми у току истраживања и навели их у одговарајућим поглављима. Може се закључити да информација представља податак који има значење.

Полазећи од наведеног, безбедност информација (а на овом месту нећемо да додатно оптерећујемо овај осврт на терминолошку неусклађеност подсећањем на теоријске дискусије које се воде око термина „безбедност“, „сигурност“, „заштита“ и сл.) односи се на заштиту информација у смислу поверљивости, интегритета и доступности.

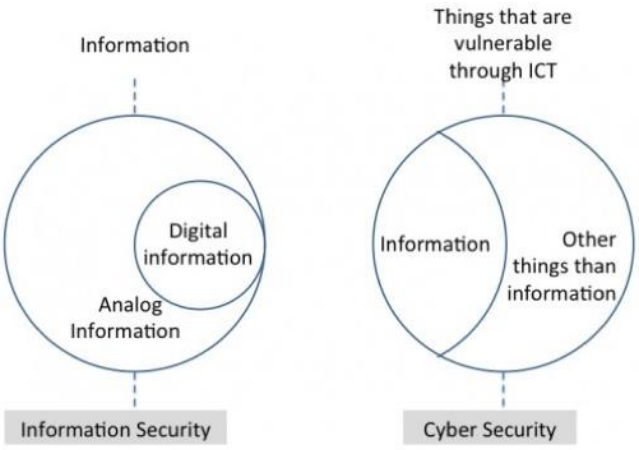
Сајбер (кибер) безбедност, односи се на заштиту рањивости које долазе из сфере ИКТ-а (информационо комуникационе технологије – ИКТ). Тако долазимо и до још једног термина у употреби, ИКТ безбедности, који подразумева безбедност података који се

[161] Доступно на: https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information?xg_source=activity

налазе у ИКТ систему (подразумева место где се подаци чувају и обрађују и технологије које се користе за ту сврху).

У циљу визуелизације изнетог, у тексту је дат Венов дијаграм односа термина: *безбедности информација* и *сајбер безбедност* (Схема број 5: *Венов дијаграм односа термина: безбедност информација и сајбер безбедност*).[162]

Схема број 5: ***Венов дијаграм односа термина: безбедност информација и сајбер безбедност***[163]



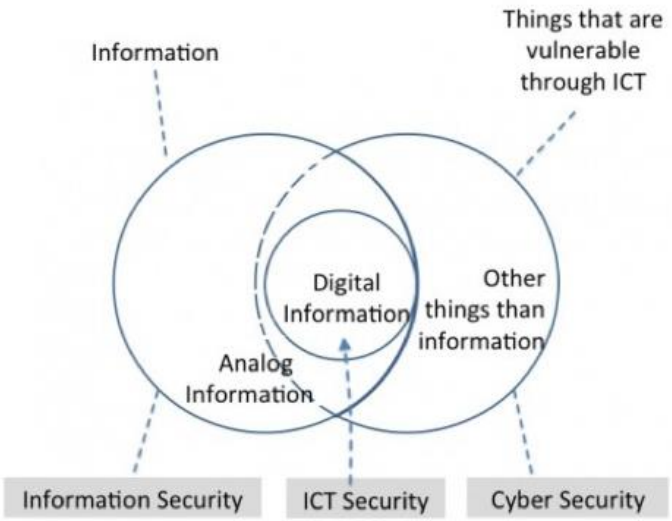
На дијаграму можемо видети да заштита информација обухвата безбедност скупова дигиталних и аналогних информација, док на десној страни видимо сајбер безбедност (ресурси који су рањиви путем ИКТ-а).

Однос обима посматраних појмова на Веновом дијаграму, асоцирао нас је на још једну терминолошку недореченост у науци и у пракси. Да ли су дигиталне информације предмет заштите сајбер безбедности или *IT* безбедности? Аутор такође спомиње ову неодређеност и закључује да *IT* безбедност подразумева заштиту информационих технологија. Практично, став је да су сајбер безбедност и *IT* безбедност синоними, наводи се у овом раду.

Можемо да приметимо да сајбер безбедност представља све ресурсе којима се може приступити путем сајбер простора. Поједностављено, на овом свету је све рањиво што је садржано у ИКТ систему, наоди се у тексту.

[162] Венов дијаграм (који се такође назива примарни дијаграм, сет дијаграм или логички дијаграм) је дијаграм који приказује све могуће логичке односе између коначне колекције различитих скупова.
[163] *Ibid*

Схема број 6: ***Венов дијаграм односа термина заштита информација, ИКТ безбедност и сајбер безбедност***[164]



Како је претходно изнето сувише велики скуп могућих догађаја, у раду се прави осврт на дефиницију сајбер безбедности, како би препознали од чега се треба заштити. У ту сврху коришћена је дифиниција коју је дао НИСТ (енгл: *National Institute of Standard and Technology – NIST*), према којој је *сајбер безбедност способност заштите или одбране сајбер простора од сајбер напада.*

Са друге стране, *Заштита информација пружа заштиту од неовлашћеног приступа, употребе, откривања, ометања, модификације или уништавања у циљу обезбеђивања поверљивости, интегритета и доступности* (у свету безбедности опште познат и прихваћен CIA принцип, када је у питању заштита информација, о чему ћемо касније у раду више говорити, означава: енгл: *Confidentiality, Integrity, and Availability – CIA*). Том приликом се подразумева следеће тумачење:

1) *интегритет*, подразумева заштиту од непрописне промене или уништавања информација и укључује обезбеђивање веродостојности информација;

2) *поверљивост*, значи очување ауторизованих ограничења приступа и откривања, укључујући средства за заштиту личне приватности и власничких података; и

3) *доступност*, значи обезбеђивање правовременог и поузданог приступа и коришћења информација.

Следећи изнето, закључује се да се сајбер безбедност односи на безбедност било чега у сајбер простору, док безбедност информација подразумева заштиту информација − без обзира на подручје (дигитално или аналогно) где се налазе.

[164] *Ibid*

Ми смо склони да просудимо, на основу претходно наведеног, да је безбедност (заштита, сигурност, итд.) информација надређени појам сајбер (кибер) безбедности.

У сваком слаучају, какав год био став о изнетим питањима, неспорно је да људи имају различите разумевање ових појмова и начелно их користе алтернативно.

Полазећи од предмета нашег истраживања, нама је посебно користан став аутора да постоје културни, па чак и политички аспекти који се тичу употребе ових термина. Подсећања ради, ми смо у хипотетичком оквиру већ наслутили да се заштита информација (па чак када се назива и сајбер безбедност, или *IT security*) не може посматрати само као техничка дисциплина, јер она зависи од многих нетехничких елемената, које можемо сусрести у области организационе културе (безбедносна свест запослених и друго).

У посматраном тексту примећује се да се у САД претежно користи термин „сајбер“ безбедност, док се у Русији претежно користи „информациона безбедност“. Историјски посматрано, информацона безбедност је била доминантан термин раније, а у време спроведене анализе, у раду се закључује, наведени термини користе се подједнако, с тим да сајбер безбедност бележи позитиван тренд (мерена су оба начина писања појма на енглеском језику).

Графикон број 5: ***Дијаграм обима претраживања појмова сајбер безбедност и информационона безбедност (енгл: cybersecurity, cyber security, and information security), на глобалном нивоу и у периоду од 2011. до 2016. године, према претраживању google search***

За потребе нашег рада, у априлу месецу 2020. године, поновили анализу учесталости претраге ових појмова, на глобалном нивоу и у последњих пет година. Установили смо да су трендови раста термина који се односе на сајбер безбедност наставили са

позитивним трендом – у толикој мери, да можемо да закључимо да је данас доминантно у употреби термин *сајбер безбедност*.

Графикон број 6: ***Дијаграм обима претраживања појмова сајбер безбедност и информационна безбедност (енгл: cybersecurity, cyber security, and information security), на глобалном нивоу и у периоду од 2015. до априла месеца 2020. године, према претраживању google search***

Објашњење ове појаве није тема нашег предмета истраживања, али може значајно да допринесе у закључним разматрањима рада. Наша је претпоставка, у мери у којој се изнети показатељи о учесталости претраге појединих појмова могу сматрати научно релевентном информацијом, да пораст тренда употребе термина сајбер безбедност, на рачун информационе безбедности, може да буде вишеструк, а да одговоре можемо потражити у следећим оквирима:

- у сајбер простору је доминантан енглески језик (лингва франка[165]), и то чак пет пута више од руског или кинеског језика и више него дупло у односу на шпански језик. У ЕУ је други језик по броју људи који га говоре и представља један од службених језика за комуникацију администрације ЕУ (поред немачког и француског); [166]
- стандарди, примери најбоље праксе и друга документа из области безбедности информација која се примењују у свету, како на енглеском говорном подручју,

[165] У онлајн верзији речника *Oxford Advanced Learner's Dictionary,* (лат: *lingua franca*) је дефинисан као језик који је усвојен као заједнички језик међу говорницима чији је матерњи језик различит. Користе га неизворни говорници, који имају различите лингвистичке и културне позадине. Не ради се о језику за посебне намене, нити о пицину или међујезику. Дакле, лингва франка је језик за комуникацију. Пицин је језик сторен на бази речника и структуре једног језика. Користи се када нема заједничког језика између група.

[166] Податке смо добили користећи сервис *google trends*. Доступно на: https://trends.google.com/trends/?geo=RS

тако и у регионима где преовладавају други страни језици, изворно су на енглеском језику. Ова чињеница се посебно одражава у сфери самоучења стручњака, одакле се у говорном стручном језику примењују појмови који долазе одавде. На тај начин се ствара „нови језик“ струке, што искуствено опажамо код *IT* струке, а посебно у Републици Србији. Последично, и термини који се користе у сајбер безбедности, потичу из тог „новог језика“ струке;[167]

- у области заштите информација, доминирају стандарди који долазе из техничког подручја, у односу на нетехничке стандарде;
- кадровска структура стручњака који се баве заштитом инфомација је таква да је њихово формално образовање углавном техничке природе (јер се безбедност информација везује за сајбер простор, оправдано или не), што је наша претпоставка коју тек треба доказати. Искуствено опажање нам говори у прилог овог тврдњи;
- нормативни оквир уређености заштите информација, када је у питању Република Србија и међународна сарадња, долази од стране институција и органа ЕУ, у највећем броју. Они стандарди и препоруке који потичу ван овог подручја, у складу са већ наведеним – на енглеском су језику, одакле се приликом превођења на српски језик све чешће користе термини створени у „новом језику“ струке;
- америчке софтверске компаније су убедљиво најбројније у свету, одакле се не може игнорисати интерес ширења тржишта и боље продаје производа (тиме и производа за заштиту информација) ове индустрије. Маркетиншки је прихватљивије област информација називати сајбер простором, јер и сами производи и услуге које нуди индустрија долазе претежно из сајбер простора;
- у САД термин сајбер безбедности (изнели смо већ да је чест синоним *IT* безбедност) је двоструко више у употреби од информационе безбедности, одакле се он последично, преко производа, трансфера знања, стандарда и друге документације која чини нормативни оквир заштите информација преноси даље, као неформални стандард струке.

Анализом коју смо обавили, установили смо да у Русији, дакле тамо где је према налазу претходног истраживања доминантно у употреби био термин информациона безбедност, сада је потпуно другачија ситуација, а термин сајбер безбедност је у

[167] Да ово није усамљен пример говори нам лингвистичко истраживање, управо у области банкарства у Републици Србији. Пронађено је више од 800 термина који се користе у банкарству (а да имају контакт са енглеским језиком) и сваки од њих је анализиран у оквиру педесет различитих лингвистичких категорија. Резултати показују да је реч углавном о преузимању термина из енглеског језика, а не о превођењу. Аутор наводи да је енглески језик лингва франка (лат: *lingua franca*) светске банкарско-финансијске заједнице, а да са друге стране наш језик има значење у комуникацији локалног типа, те да је под снажним утицајем енглеског језика, али и да га краси небрига од стране корисника. Резултат истраживања је речник у којем је садржано око 400 стандардизованих термина српског језика банкарства и финансија – дакле предлог термина које нема потребе изговарати на страном језику, што је половина термина обухваћених истраживањем. Више о томе: Вулетић, Ђ. А.: *Контакти енглеског и српског језика у области банкарства и финансија*, докторска дисертација, Филолошки факултет, Универитет у Београду, Београд, 2013. године, доступно на: http://nardus.mpn.gov.rs/bitstream/handle/123456789/4044/Disertacija.pdf?sequence=1&isAllowed=y

изражено чешћој употреби од информационе безбедности, што опет може довести до даљих закључака у смислу прогнозе кретања трендова о питању „да ли сајбер (IT) или информациона безбедност (или заштита)“.

1.2. Информација и информатичко доба

У теоријским радовима постоје различите дефиниције појма информације. О томе је сагласан и Путник, који износи став да је информација постала релевантан појам за све науке које се баве симболичком комуникацијом, у распону од математике до рачунарске науке, или од логике до лингвистике, односно од електронике до библиотекарства, као и од хуманистичких наука и уметности до документаристике, али и од друштвених наука до медицине. То је информацији дало интердисциплинарну димензију, јер је свака наука покушала и још покушава да протумачи тај комплексан појам. Све ово нам говори да појам „информација“ није лако схватити нити једноставно протумачити[168].

Мандић препоручује да се у том смислу посматрају две дефиниције: да је информација функција односа изумеђу могућих одговора пре и после пријема поруке (Луј-Марсел Бриљон) и – да је информација назив за садржај који је размењен са спољашњим светом у поступку усаглашавања са њим (Норберт Винер)[169].

Реч „информација“, изведена је из латинске речи *informatio*, што значи, порука, скуп, спознаја, представа. Појам информације би се могао одредити као садржај о одређеном догађају, појму, збивању, процесу који отклања неку неодређеност и на тај начин увећава сазнање, а увек се креће од обавештенијег субјекта ка примаоцу нижег нивоа обавештености. Према Шафранском, информација је „садржај или значење поруке“. Информације се генеришу (и/или перципирају) као визија (слика), звук, укус, мирис и све остало што прихватају људска чула.[170]

У пракси се често може чути замена термина „појам“ и „информација“, и ако се у сушини не ради о синонимима.

„Важно је начинити разлику између податка и информације, појмова који се често поистовећују. На пример, број 6 је податак и он као такав нема посебно значење, међутим, „Сада је 6 часова“ јесте информација, јер је податку додељено неко значење. Тако можемо увидети да се информација састоји од податка и значења које му је додељено“[171]. Такође, о овоме се може дати и објашњење да подаци могу бити било који карактер, текст, слика, звук, али ако се не стави у контекст, значи врло мало илико

[168] Путник, Н.: Кибер ратовање – нови облик савремених друштвених конфликата, докторкса дисертација, Факултет за безбедност, Београд, 2012, стр. 63 - 74

[169] Дато према: Цигурски, О.: *Информатика*, Факултет цивилне одбране, Београд, 2002, стр. 41.

[170] Вулетић, Д.: „Шта је информационо ратовање?“, *Безбедност*, бр. 3/05, Београд, 2005, стр. 494.

[171] Путник, Н, *op.cit*, стр. 64

скоро ништа за човека. Информација је корисна и обично форматирана на такав начин да је разумљива за човека. [172]

Историјски посматрано, у развоју информације и њеног утицаја на живот модерног човека можемо разликовати неколико периода.

Половином деветнестог века дошло је до појаве иновативних техничко-технолошких достигнућа који су омогућили квалитативан помак у начину и брзини преношења информације (телеграф, радио и телефон).

Средином XX века, за развој информације је важна појава телевизије, прве генерације рачунара и сателита. Овим средствима постало је могуће, у односу на претходни период, пренети већи број информација у ефикаснијем формату (телевизија). Такође, омогућена је већа могућност сакупљања, анализе и употребе информација (рачунари), а створила се и глобална инфраструктура телекомуникација (сателити).

Крајем XX века, развијени су персонални рачунари и рачунарске мреже. Развој и примена и информатике и информационих система надмашили су све оно што је у претходном периоду постигнуто, у делу размене информација, па се на тај начин овај период извдојио као нова етапа, или Трећа информатичка револуција. Овај период се заснива на осам технолошких достигнућа, и то:[173]

- унапређени су полупроводници;
- рачунари нове генерације;
- оптичка влакна;
- мобилна телефонија;
- сателитска технологија;
- мрежно повезивање рачунара;
- унапређена интеракција човек-рачунар;
- дигитални пренос.

Ове технологије се све заједно називају информационо-комуникационе (ИКТ) технологије. Свака од њих побољшава способност коришћења и размене информација, чиме се избегава ограничење времена, раздаљине и позиције.

Резултат оваквог развоја довео је до:

- веће брзине преноса информација;
- бољег вођења, обраде и тумачења великог броја информација (што резултира ефикаснијем одлучивању);
- флексибилности тока информација (информација се може истовремено објављена на више локација; може бити примљена из више извора; може се одвијати само између заинтересованих коресподената);
- веће могућности приступа информацијама.

[172] Доступно на: http://www.computerhope.com/issues/ch001629.htm
[173] Путник, Н.: *op.cit.*, стр. 65

Достигнућа Треће информационе револуције, заједно са развојем глобалне рачунарске мреже – Интернета, променила су економску, политичку и кутурну сферу друштвеног живота, тако да тако данас многи аутори говоре о „информационом друштву“.

Путник закључује, на основу прегледа домаће литературе, да је у нашем језику чешћа употреба термина „информатичко“ од „информационо“. У том смислу он наводи став Букумировића, да је у англосаксонским земљама некада коришћен термин „*computer science*“, а да је данас у примени термин „*information science*“. У Википедији се наводи да неки аутори сматрају да је информатика синоним за науку о информацијама. Флеч наводи да термин „информационо друштво“ имплицира централну улогу информације. Информације су одувек представљале важан фактор у развоју света, разлика је што данас расположемо ИКТ средствима (информационо комуникационе технологије), која омогућавају много боље перформанске у обради и дистрибуцији информација и знања.[174]

1.3. Историјски развој информацине безбедности

Опште је прихваћено да су значај информација људи препознали од почетка развоја људске заједнице.[175] За потребе нашег рада ми ћемо приказати историјски развој, условно названо, модерне информационе безбедности, која почиње када и појава рачунара.

Првобитно су то биле потребе да се физички обезбеде локације где се рачунари налазе, као и њихов софтвер и хардвер. Обично се за почетак овог развоја узима Други светски рат, када су постављени основни оквири рачунарског развоја, праћени захтевом да се разбију комуникацијски кодови зараћених страна. Познати су догађаји око разбијања кода Енигме, чиме је обележен почетак развоја информационе безбедности.[176]

---

[174] Путник, Н., *op.cit.*, стр. 67 – 69.

[175] Више о томе: Krieger, W.: *Историја тајних служби – од фараона до НСА*, Лагуна, Београд, 2016. година

[176] Енигма је шифарска машина коју је изумео немачки инжењер Артур Шербијус (нем: Arthur Scherbius) пред завршетак Првог светског рата. Скоро истовремено су три различита проналазача, из три различите земље, поднела своје патенте за ротирајуће шифарске машине (Edward Hebern, Arvid Damm, Hugo Koch). Шербијус је на почетку производ намењо комерцијалног употреби, будући да војска није била заинтересована за њену примену. Тек средином двадесетих година прошлог века, и уз неколико еволуција првобитног модела (увек се побољшавао ниво шифровања), немачка војска је показала заинтересованост за овај производ, да би 1930. године, почели да наручују овај производ. Основни принцип код Енигме је у знаковној супституцији (земени откуцаног слова другим), што значи да је сваки знак отвореног текста (улазног текста) замењен другим знаком (излазног текста). Преко немачког шпијуна (Hans-Thilo Schmidt), Француска се домогла шифарске књиге коју је проследила Британији и Пољској. Пољски биро (Biuro Szyfrow) је успео да „пробије“ Енигмине поруке, користећи математику (Marian Rejewski, Henryk Zygalski i Jerzy Rozicki). Они су развили и прву електромеханичку машину „Бомба“, како би убрзали процес разбијања Енигме. Када је почела инвазија на Пољску, немци су додали два нова ротора, и на тај начин су повећали број комбинација са 6 на 60 пута, што је пољску „бомбу“ начинило неефикасном. Пољаци су своја сазнања проследили британцима и французима 1939. године, а Алан Туринг, британски математичар, је на другачијем принципу у односу на „бомбу“,

Растућа потреба за безбедности на националним нивоима довела је до сложенијих и технолошких софистицираних заштитих мера рачунара. Током тих раних година, безбедност информација базирала се на мерама физичке заштите и класификацији докумената.[177]

Шездесетих година прошлог века организације су почеле да штите своје ралунаре лозинком. Тада није било интернета, или мреже за коју би се требало бринути, па је безбедност усмерена на физичке мере и спречавање приступа људима који имају довољно знања да би евентуално могли да раде на рачунару. Из тих разлога су уређајима додате лозинке и више слојева безбедносне заштите.

Седамдесетих година, историја информационе безбедности настављена је када је Боб Томас (енгл: *Bob Thomas*) успео да направи програм којим је успео да уђе у пројекат Арпанет (енгл: *The Advanced Research Projects Agency Network − ARPANET*). Програм је назвао Крипер (енгл: *creeper*), према поруци коју је остављао програм где год се кретао у тој мрежи (енгл: *I'm the creeper – catch me if you can*). Реј Томлисон (енгл: *Ray Tomlinson*), човек којем се приписује проналазак *E* поште, касније је осмислио програм који је Крипер подигао на виши ниво, чинећи га самореплицирајућим и првим икада направљеним рачунарским црвом. Срећом, написао је и програм Рипер (енгл: *Reaper*), који се успешно супротставио Криперу, и на тај начин је написао и први антивирусни софтвер. Значај ових програма је у томе што су показали мрежну рањивост Арпанета, у доба када су многе организације и владе повезивали своје рачунаре телефонским линијама, да би створили сопствене мреже. Многи су у то време покушавали да пронађу начин да се инфилтрирају у такве мреже и да украду поверљиве податке. Тако су рођени и први хакери на свету.

Осамдесетих, рачунари су почели све више да се повезују. Рачунарски вируси су постали напреднији, а информатички безбедносни системи (већ) нису могли да држе корак са сталним и иновативним приступом хаковању. Англосаксонски извори наводе да су „руси први почели", тако што су ангажовали немца, хакера, Маркуса Хеса (енгл: *Marcus Hess*), да од американаца украде одређене војне тајне. Хес је упао у преко четири стотине војних рачунара, укључујући и оне у Пентагону, са намером да ово прода КГБ-у (осујећен је, кажу извори). Две године касније, рођен је Морис Ворм (енгл: Morris Worm), један од важнијих догађаја у историји информационе безбедности. Мреже су нагло почеле да се шире, као и круг корисника (универзитети, војске, владе и други). Последица је била да су мере безбедности морале да се такође „шире", што је направило могућност за рађање Мориса Ворма. Овај рачунарски црв је осмислиио Робер Морис (енгл: *Robert Morris*), тако да се он ширио по мрежама и том

осмислио заједно са својим тимом 1940 године нову машину која је могла да дешифрује Енигму коју је користила авијација, док је за морнаричку верзију машине требало више времена, што су успели након заробљавања немачке подморнице U-110, на којој се налазила шифарска књига Енигме. Цео текст је доступан на: https://raf.edu.rs/citaliste/istorija/4336-enigma

[177] Introduction to Information Security, доступно на:
https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf

приликом се сам копирао, на тако агресиван начин да је изазивао успорење рада интернета – готово до престанка његовог рада, чиме су изазвана и бројна оштећења. Проурокована штета је била толика да је Морис постао прва особа која је оптужена према Закону о компјутерсим преварама и злоупотребама. Резултат је био и формирање рачунарског ЦЕРТ-а, Тима за хитне случајеве (енгл: *Computer Emergency Response Team – CERT*), како се овакве штете не би поновиле. У току овог периода Арпанет је постао познатији и као Интернет, који је постао дуступан широм света 1989. године.

Деведесетих је интернет постао доступан јавности, тако да је све више људи почело да оставља своје личне податке на мрежу. Организовани криминал је ову могућност препознао као нови извор прихода, одакле је почео и масовнији развој овог вида криминала. Већ средином ове декаде, претња мрежној безбедности је експоненцијално порасла, одакле су се развили фајерволи и антивирусни програми (енгл: *firewalls and antivirus programs*), али не толиком брзином колико су хакери напредовали у својм вештинама.

Двехиљадите, обележиле су активности влада да сузбију хаковање као облик криминала, тако што су одредили строжије казне починиоцима. Информациона безбедност је наставила да се развија, као и сам Интернет, али то важи и за вирусе.

Последња декада, бележимо стални развој технологије, али и хаковања. Инциденти изазвани злонамерним активностима су постали све чешћи, све обимнији и са више нанете штете. Најпознати су: Афера Сноудена са Националном безбедносном агенцијом, НСА (енгл: *Edward Snowden & National Security Agency − NSA*), 2013. године, бивши запослени ЦИА-е (енгл: *CIA*), копирао је и објавио податке НСА, исгичући чињеницу да је влада шрijунирала јавност; Yahoo, 2013. – 2014. године, хакери провалом угрозили рачуне и личне податке великог броја корисника, због чега је компанија кажњена са 35 милиона долара (нису благовемено објавили компромитацију података), а цена компаније је на берзи опала за 350 милиона долара; *WannaCry,* 2017. године, напад је општепознатији као први рансомворм (енгл: *ransomworm*), где су мета били рачунари са Мајкрософтовим Виндоус оперативним системом (енгл: *Microsoft Windows operating system*), где се откупнина плаћала у криптовалути Биткоин. За само један дан, заражено је преко 230 хиљада рачунара у 150 земаља.[178]

1.4. Вредност информације

У области заштите информација често се говори о вредности информација, па у том смислу можемо констатовати да штитимо оне информације које класификујемо као поверљиве. Организације некада саме одређују вредности својих информација, и у том

[178] Доступно на: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

смислу можемо говорити о информацијама које су више вредне од других. Једна иста информација у различитом временеском оквиру може заузимати различите вредности, а слично је и са контекстом у којем се она пласира. Тако на пример, информација о окупљању навијача пре неког јавог догађаја може бити информативног и необавезујућег карактера за јавност, али истовремено може бити и поверљива, уколико је реч о укупљању такозваних навијачких група у време друштвено важног догађаја (грађанских протеста, политичких скупова, различитих манифестација и друго), у извештајима које анализира неки орган безбедности.

Организације, природно стално анализирају информације које се односе на њихову привредну делатност, па тако посматрају скупове информација са којима располажу и на основу тога доносе пословне одлуке.

Поред наведеног, и државни органи због своје заинтересованости за стабилност економског система, која не може да се постигне уколико и субјекти нису стабилни, а они опет не могу да буду стабилни у условима прекомерног угрожавања пословања, често својим формалним одлукама утичу на привредне субјекте да своје информације, у складу са њиховом вредности, чувају на оређени начин. Одатле потиче формална категоризација одређених информација.

Тако, се у *Закону о банкама* наводи да се подаци који се односе на контролу бонитета и законитости пословања банке, као и о реструктуирању, одређују као тајни подаци са ознаком степена тајности „строго поверљиво“, поверљиво“ и „интерно“.[179]

Закон о тајности података, препознаје категорије „државна тајна“, „строго поверљиво“ или „интерно“.[180]

Да би информације могле да се вредносно категоризују, организације су принуђене да направе њихов попис, да дефинишу власника информација, да одреде њихову вредност за организацију и да формулишу правила на који начин се оне складиште, чувају од неовлашћеног приступа, како се врши њихова дистрибуција, како се уништавају и слично.

Ми смо становишта да на категоризацију информација, у смислу њихове поверљивости, утичу једнако амбијент у којем се налази организација (вредносни систем, општа култура, безбедносна култура, нормативни оквир од стране Владе или од надлежних министарстава и других државних институција, нормативни оквир који ствара међународна заједница и друго), као и околности које ствара сама организација (природа делатности, организација рада, организациона култура, нормативна уређеност, безбедносна свест запослених и друго).

Променљивост временског оквира и контекста у којем нека информација зузима своју вредност, наводи нас на закључак да је она динамичка категорија, у којем може да

[179] Закон о банкама, народна Банка Србије, 2015. година, Члан 96, доступно на: https://www.nbs.rs/internet/latinica/20/zakoni/kpb_banke_2015.pdf
[180] Закон о тајности података, „Сл. Гласник РС“, бр. 104/2009, Члан 2, став 6

заузима различите вредности: од оних које су опште и јавно доступне информације, до оних које су поверљиве – и обрнуто.

У циљу заштите поверљивих информација у организацијама се дефинише *Правилник о пословној тајни*, као формални документ са којим треба да су упознати сви запослени, будући да су у њему одређене обавезе запослених у овом смислу, као и евентуалне казне за непоштовање прописаних правила.

Мандић наводи да се вредност пословне информације везује за одлучивање и управљање у организацији, као и да њена вредност зависи од неколико њених особина, и то:[181]

- актуелности;
- тачности;
- поузданости;
- трајности;
- расположивости;
- мере у којој задовољава потребе корисника.

Систем пословних информација у организацији треба да садржи следеће елементе:[182]

- прикупљање и проверу података из извора који се налазе у и ван предузећа;
- смештај и чување, односно "меморизацију" података за каснију употребу према потреби;
- проналажење и обраду ускладиштених података који на овај начин постају пословне информације; и
- дистрибуцију и коришћење пословних информација за доношење одлуке

Мишљења смо да овоме треба додати и сегмент уништавања пословне документације (информација), посебно полазећи од процеса дигитализације, где се информације налазе на различитим медијима. Банке и друге финансијске институције, поред информација које чувају на папиру, у власништву су и информација које се налазе на радним станицама запослених. Процес замене рачунара, треба да предвиди на који начин се обавља пренос података на нову меморију, како се подаци бришу са хард дискова који се мењају, како се они чувају, и на крају – која је процедура за њихово механичко уништавање (прављење нечитљивим за дигиталну форензику). Ове организације имају обавезу архивског чувања појединих докумената који су направљени у папиру (на пример: уговори са корисницима, документација отворених рачуна, депо картони и друго), па је у том смислу неопходно и овај аспект заштите информација регулисати интерним актима и процедурама.

Даље, Ранђеловић наводи да је информација нешто што смањује или укида неуређеност система, односно смањује неизвесност промена – одакле такође видимо

[181] Мандић, Ј. Г.: *Системи обезбеђења и заштите*, Факултет цивилне одбране, Универзитет у Београду, Београд, 2004. година, стр. 207.
[182] *Ibid*, стр. 208.

особину вредности. Овај аутор наводи да је постоји мера *ентропије информација,* која подразумева мере неорганизованости система, нереда у њему и меру неизвесности о подацима у пренетим порукама.[183]

За потребе нашег истраживања, ми нећемо даље разматрати теоријске поставке које говоре о вредности информација, посебно јер ће неки аспекти, као што је нормативно уређење области заштите инфомрација у банкама и финансијским институцијама, где се као што смо претходно видели на регулаторан начин штити вредност информација, бити посебно разматрано.

1.5. Информациона безбедност

Не постоје никакве сумње у велики значај које за развој савременог друштва имају информације. Потреба за информацијом и знањем сматра се једним од најбитнијих обележја савременог света. Информација и знање су, међутим, одувек били битни ресурси за човечанство – у толикој мери да је мања или већа могућност приступа и преношења иноформација могла да, током историје, одреди успех или неуспех цивилизација и култура[184].

Извесно је и да је једна од карактеристика тржишта немогућност пословања без технологије, а она опет не би била потпуна без информационе технологије (*information technology – IT*). Пословни свет све више увиђа значај заштите таквих ресурса, одакле се последично развија и свест о потреби заштите информација (*information security – IS*). Међутим, истовремено расте и свест о томе да питање заштите информација није само техничко питање. Потребно је да у том процесу учествују три различите групе „доносиоца одлука“ (*decision makers*) – са заједничким интересом, и то:[185]

- стручњаци (менаџери) за заштиту информација;
- *IT* менаџери;
- пословни менаџери (нетехничко особље).

Кроз процес међусобне дискусије ове три групе треба да пронађу свеобухватан план за заштиту информационих добара, на таква начин да свака испуњава своје задатке који се односе на:

- менаџери заштите информација, да заштите информациона добра од многих претњи;

[183] Ранђеловић, Д.: *Основи информатике*, Криминалистичко-полицијска академија, ЈП „Службени гласник“, Београд, 2013. година, стр. 25.
[184] Путник, Н.: *Сајбер простор и безбедносни изазови*, Факултет за безбедност, 2009. година, стр. 15
[185] Whitman, M., Mattord, H. J.: *Management of Information security*, Course Technology Cengage Learning, second edition, Boston, USA, 2008., pg. 2-5

- IT менаџери, да у свом домену подржавају достизање пословних циљева и потреба;
- пословни менаџери (нетехничко особље), одређују и повезују организациона правила и политике и проналазе одговарајуће ресурсе у оквиру организације.

Мандић[186], наводи да је систем безбедносног менаџмента из области система обезбеђења лица, имовине и пословања (СОЛИиП) интегрална компонента општег менаџмента на највишем ниову хијерархије који:

- дефинише и одређује захтеве и потребе система обезбеђења, самостално и у сарадњи са осталим руководним структурама;
- остварује процес планирања потреба;
- обезбеђује организацију, реализацију и имплементацију планираног, кроз одлучивање, вођење, координацију и контролу (ових послова);
- омогућава непосредно и посредно извршавање задатака, активности и делатности постављених пред систем обезбеђења ради постизања његове примарне функције - заштите имовине, лица и пословања.

Комуникација између менаџмента из области СОЛИиП-а, и општег менаџмента, односно како то наводе у трипартитној подели *Whitman* и *Mattord*[187], када говоре о *decision makers*-има, у области заштите информација – „пословних менаџера“, треба да буде таква да општи менаџмент при доношењу одлука уважава постулате СОЛИиП-а, а да менаџери СОЛИиП-а не смеју да својим предлогом одлука успоравају и угрожавају остале активности предузећа. Ова повезаност усложњава функционисање управљања људским ресурсима и даје специфичности безбедносном менаџменту у односу на друге облике менаџмента.[188]

Слично, како смо дискутовали у опису феномена безбедности код домаћих аутора (Даничић и Стајић[189]), када смо навели да се приватна безбедност може посматрати кроз системски приступ, Whitman и Mattord наводе да се уопштено безбедност треба посматрати као процес истовремених примена неколико различитих стратегија. Свака та стратегија има свој приступ, са аспекта своје специјализованости за одређени део мера безбедности. Као пример таквих специјализација они виде следеће области: [190]

- физичку безбедност, обухвата стратегију за заштиту људи, добара и радног окружења, укључујући различите претње као што су пожар, неовлашћени приступи и природне несреће;
- безбедност пословања, обухвата стратегију коју треба да омогући способност организације да обавља своје активности без прекида;

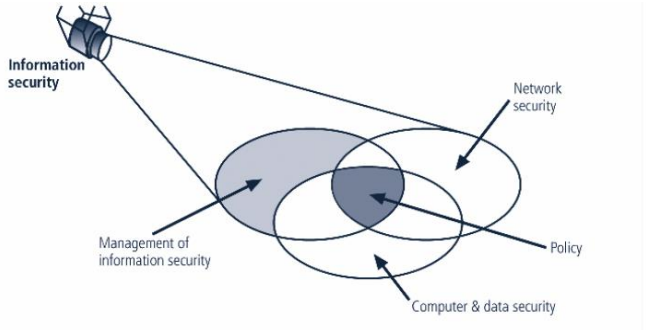
[186] Мандић, Ј. Г.: *Системи обезбеђења и заштите*, стр. 173. – 174.
[187] Whitman, M., Mattord, H. J, *Ibid*
[188] Мандић, Ј. Г, *Ibid*
[189] Даничић, М., Стајић, Љ.: *Приватна безбједност*, Висока школа унутрашњих послова, Бања Лука, 2008, стр. 20.
[190] Whitman, M., Mattord, H. J., *Ibid*

- безбедност комуникација, обухвата стратегију заштите свих ресурса који служе за комуникацију организације, укључујући технологију;
- *network security*, обухвата стратегију заштите мрежних уређаја и веза.

Свако од наведених подручја доприноси информационој безбедности у целини, а овакав став је дат на основу стандарда који је издао Комитет за национални систем безбедности (*Committee on National Security Systems - CNSS*), раније познат као Комитет за национални систем безбедности телекомуникација и заштиту информација (*National Security Telecommunications and Information Systems Security Committee – NSTISSC*).

Ови аутори закључују, да је Информациона безбедност (*Information security – InfoSec*) заштита информација и критичних елемената, укључујући њихов хардвер (*hardware*) који користе за складиштење и пренос података, путем примене процедура (*policy*), одговарајућих обука, те подизања свести о информационој безбедности (*security awareness program*).

Схема број 7: *Компоненте система информационе безбедности*[191]



Информациона безбедност обухвата широке области: менаџмент заштитом информација, заштиту рачунара и података и *network security*. У самом центру овог система је концепт одговарајућих политика и правила (процедура). Може да се закључи да су процедуре (безбедносна правила/политике), безбедносна свест (*security awareness)*, едукација (оспособљавање), тренинг и технологија, витални садржаји за заштиту информација (Схема број 7: *Компоненте система информационе безбедности*) .

1.6. Мере и стратегије заштите информационих система

Разматрајући питања угрожености информационих система, Петровић наводи да је експанзија информационе технологије представља истински феномен данашњице,

[191] Прилагођено према: Whitman, M., Mattord, H. J, op.cit., стр. 5

будући да са једне стране она омогућава низ погодности, док, са друге стране, уочавамо читав низ проблема и ризика. [192] У том смислу, овај аутор, после изношења ретроспективе проблемског разматрања ове врсте заштите у свету, иако том приликом разматра период осамдесетих година прошлог века, даје методолошки допринос у стварању система заштите, због чијег значаја, имајући у виду наш предмет истраживања, желимо да му посветимо детаљније објашњење.

Полазећи од „златних питања криминалистике“[193], овај аутор поставља следећа питања:

- шта штитимо;
- од кога (од чега) штитимо;
- због чега штитимо;
- чиме штитимо;
- како штитимо.

На тај начин Петровић поставља главне ентитете заштите у области информационих система, као: објекте заштите, претње (идентификацију опасности), утрђивање могућих последица и – мере заштите.

Објекте заштите чине:

- подаци;
- датотеке;
- базе података;
- оптичке слике;
- докумената;
- дигитални запис звука;
- софтвер;
- програми;
- централна јединица;
- периферни уређаји;
- екстерне меморије;
- терминали;
- персонални рачунари;
- листинзи;
- документација;
- локација за смештај.

[192] Петровић, С.: *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004.
[193] Алексић, Ж., Миловановић, З.: *Криминалистика*, Партенон, Београд, 1994, стр. 50

Овакав скуп може да послужи као полазна основа, која би се у зависности од конкретних услова сузила или смањила. Даље, сваки од овако датих објеката може се разложити на објекте нижег нивоа. Тако, ако посматрамо *податке,* и узмемо у обзир њихову тајност, можемо из разложити на општу и посебну категорију. Посебне податке можемо даље разложити на научне, пословне, војне, полицијске, личне и слично.

Претње – опасности, представљају практично наограничен скуп могућности. Информациони системи су подложни свим класичним ризицима, као што су ватра, вода, експлозија и сл., али и специфичним ризицима, као што је електромагнетно зрачење. Међу појединим претњама постоји одређена међузависност, која условљава да појављивање једне претње иницира и појављивање друге претње, као и да повећање интензитета једне аутоматски утиче на повећање ове друге. Највећи проблем у разматрању претњи је чињеница да се претња која није идентификована може касније показати као катастрофална. Због тога се оправдано поставља питање методолошког приступа, где у теорији не постоји јединствен став. Не разматрајући на овом месту посебно овај проблем, можемо рећи да је разврсавање у групе, које представљају логичке групе, може само да олакша анализу – а све у зависности од циља који пред собом истраживачи имају.

Аутор	Група претњи
Палмар и Потер[194]	– Деструкцију добара – Неовлашчену модификацију или манипуплацију информацијама – Неовлашћено откривање информација – Спречавање коришћења добара – Преваре
Јаворовски[195]	– Обрада података – Трансфер података – Отицање података – Административне процедуре – Персонал – Физичке области – Операције (активности)
Молема и Смулдерс[196]	– Неовлашћена људска манипулација – Људске грешке – Логичке грешке – Технички недостаци – Проблеми амбијента

[194] Palmar, I., Potter, G.: *Computer security risk management*, Jessica Kingley Publishers, London, 1989, pg. 210
[195] Javorovski, M.: *Tandem threat scenarios: a risk assessment approach*, Datapro on CD, Originating Report IS 20-300-101, February 1994.
[196] Mollema, K., Smulders, P.: *Prerequistes for data control*, Computer & Security, vol 8, no. 4, pg. 320

Велашевић[197]	– Физички хазард – Неисправна опрема – Софтверске грешке – Људске грешке – Намерне повреде – Криминални акти – Инвазија приватности

На основу ових приступа, Петровић је извршио разврставање претњи у четири групе, којом приликом сам ставља ограду и износи став да постоји могућност проширења ових група, било додавањем нових било уситњавањем постојећих[198].

Ове групе су: „виша сила“ (као што су: земљотрес, поплава, друге елементарне непогоде, ванредне прилике и ратно стање); „харведрско-софтверски недостаци“ (као што су: испад система и различите техничке и логичке грешке); „људски фактор“ са атрибутом ненамерности (лоша организација, недисциплина, немар, нехат, нестручност, монотинија и замор) и - „људски фактор“ са атрибутом намерности (крађе, преваре, проневере, фалсификовање, изнуде, уцене, нарушавање приватности, саботажа, одавање тајне, шпијунажа, порнографија, пропаганда, вандализам, тероризам, убиства, хакинг, стварање и дистрибуција вируса, пиратство софтвера, ускраћивање сервиса (*DoS* напади), електронско узнемиравање и крађа рачунарских услуга).

Последице, такође у зависности од теоријског приступа могу различито да се класификују. Овај аутор предлаже такву поделу где су критеријуми: степен оштећења (уништења) објеката, хардвера, софтвера, програма, података, извештаја и документације); отуђење ових истих елемената; њихова модификација; успоравање или обустављање радног процеса – и, компромитација тајности. Све ове последице се могу исказати кроз нарушавање: интегритета (тачност и комплетност информација), расположивости (континуитет услуга) и поверљивости (осетљивост на откривање података).

Мере заштите, могу се према својој природи разврстати на следеће мере[199]:

- нормативне мере (правне, организационе, кадровске); овим мерама утврђује се политка заштите („кућни ред“), која одређује шта се сматра прихватљивим и какве су санкције за неприхватљиво понашање. Истовремено представљају средство у спречавању и откривању недозвољених понашања и активности;

- физичко-техничке мере; карактеристика им је да подразумевају инвестиције пре него што почну да дејствују (а овоме треба додати и трошкове текућег одржавања). Позитивна страна је што се ови трошкови могу проценити (планирати). У

[197] Велашевић, Д.: *Заштита података у рачунарским системима*, ЈИСА Инфо, год. 4, бр.1, 1996., стр. 5 - 6
[198] Петровић, С., *op.cit,* стр. 20
[199] Петровић, С., *op.cit,* стр. 22

амцијенту у којем нормативне мере нису примењене на адектватан начин, мере физичко-техничке заштите не морају бити ефикасне;

– логичке мере; врло су ефикасне, али повлаче за собом трошкове који се не виде одмах, јер утичу на смањење расположивости и ефикасности рачунарских система. Из ових разлога овим мерама мора да се приступа одговорно, осмишљено и рационално. И у овом случају важи да је ефиканост мера условљена адекватном применом мера нормативног карактера.

На основу изнетог, следи закључак да се при конципирању концепта заштите информационих система треба кренути од нормативних мера. „Од њих треба почети, максимално их користити и са њима треба прекрити цео информациони систем, независно од нивоа заштите који се захтева. Такво стање треба доградити физиичко-техничким и логичким мерама заштите у мери која ће обезбедити жељени ниво заштите, који може бити, на пример, стандардни, средњи, виши или највиши ниво, у зависности од потреба конкректног информационог система. Ово утолико пре што анализе бројних примера компјутерског криминала управо указују да се у највећем броју познатих случајева постојеће слабости у примени мера нормативног карактера омогућавале и олакшавале реализацију ове врсте криминалних дела.“[200]

Политика заштите, даје одговор на питање како заштити неки информатички ресурс и представља у својој суштини *управаљање ризиком*. Станг[201] наводи да су основни циљеви управљања ризиком следећи:

– Заштита система од губитака који могу угрозити циљеве због којих је он и формиран
– Смањење очекиваних трошкова предузимања мера заштите
– Смањење губитака изазазваних претњама које су реализоване, и поред предузетих мера заштите

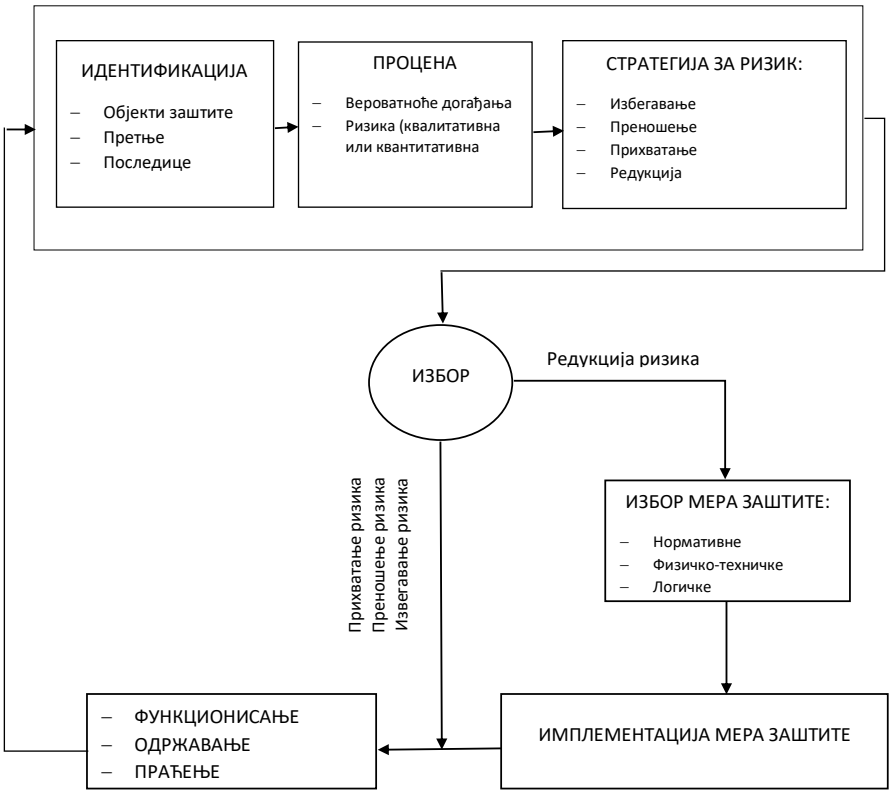
За потребе нашег рада, и на основу до сада изнетог од овог аутора, ми ћемо графички приказати општи модел управљања информационим ризиком (Схема број 8).[202]

Путник, сматра да се под заштитом информација подразумева примарни, базични ниво заштите. „Овај ниво ниво се односи на заштиту информационих система, информација и информационих мрежа у приватном власништву грађана и свим битним државним и приватним организацијама. Информације, информациони системи и мреже представљају важну имовину која има материјалну и употребну вредност за сваког појединца и сваку организацију. Информација и информациона инфраструктура могу бити од пресудне важности за очување: националне безбедности, приватности појединаца али и конкурентности предузећа и других аспеката пословања (готовинских токова, исплативости, правне усаглашености и пословног угледа). Заштитом информација од

[200] Петровић, С., *op.cit,* стр. 22
[201] *Ibid*
[202] Петровић, С., *op.cit,* стр. 36

широког опсега претњи се, са аспекта корпоративне безбедности, осигурава континуитет пословања, са циљем да се губици у пословању сведу на минимум“. [203]

Схема број 8: ***Општи модел управљања информационим ризиком***



Од посебног значаја за наш предмет истраживања су ставови Џигурског[204], који наводи да са аспекта националне безбедности, у циљу супротстављања активностима кибер ратовања, неопходно спроводити заштитне мере на следећа три нивоа:

- *оперативни ниво* – подразумева примену најсавременијих средстава за заштиту података и информатичких ресурса, код свих корисника ИК технологија. Осим тога, потребно је спроводити честа тестирања информационих система и одмах уклањати уочене безбедносне проблеме;
- *производни ниво* – развити средства за мониторинг и аутоматску проверу безбедности код произвођача информатичких средстава. Спроводити ригорозна

[203] Путник, Н., *op.cit*, стр. 368
[204] Џигурски, О.: *Информационе технологије у борби против тероризма*, Зборник Факултета цивилне одбране, Београд, 2005, стр. 179.

тестирања хардвера и софтвера информационих система на безбедносне пропусте;

- *државни ниво* – реализовати критичне државне информационе системе као високо безбедне моделе. Увести политику заштите информација и информационих система и мрежа која би се спроводила на сва три наведена нивоа.

Опсег безбедносних претњи и технике напада се усавршавају, а сами напади постају све учесталији, амбициознији и софистицираниј.

Да би се поменуте претње предупредиле, на примарном нивоу заштите морају се у обзир узети различити аспекти заштите. На основу досадашњих искустава, тзв. *добре праксе,* може се рећи да је пожељно примењивати модел вишеслојне заштите. Он представља вид проактивног деловања и обухвата неколико аспеката:

- физички (онемогућава физички приступ - физичко обезбеђење);
- технички (техничко обезбеђење - електронско обезбеђење; заштита од електромагнетног зрачења; идентификација, верификација и ауторизација приступа; системи за детекцију и спречавање напада; криптографија);
- организациони (организациона структура, дефинисање радног процеса, развој софтверских система, праћење смерница и стандардâ, планирање итд);
- кадровски (планирање и избор кадрова, руковођење, стручно усавршавање и безбедносно образовање итд.) и
- нормативни (закони, упутства, планови и друга регулатива која обавезује и прописује извршење неке радње и начин изршења те радње).

Сфере физичке и техничке заштите се, како наводи Путник, називају *техничким аспектом* заштите, док се организациона, кадровска и нормативна сфера подводе под *друштвени аспект* заштите. Оба аспекта су подједнако значајна и само се њиховом комбинацијом, и синергијским ефектом, може постићи задовољавајући ниво заштите информационих система.

Ми смо мишљења да се оваква подела, на технички и друштвени аспект заштите може прихватити само условно, будући да искутвено опажамо да иначе у стручном делу јавности не постоји јединствен став о томе шта су то техничке мере заштите, па би то онда могло довести до додатних нејасноћа (о којем виду заштите дискутујемо). Реч је о томе да је у домаћој литератури уобичајена подела у области *security* послова на (најмање) физичку и техничку компоненту. Том приликом када се говори о физичкој компоненети мисли се на послове физичко-техничког обезбеђења, а (само) техничка компоненета обухвата (техничка) средства која су у функцији остваривања циљева заштите (контрола приступа, против провала и друго).

Савремена пракса под пословима физичке безбедности подразумева, не само послове физичко-техничпког обезбеђења, него и средства која су у том циљу ангажована, укључујући и техничка средства заштите, одакле се под термином физичка безбедност (*physical security*) подразумева свеукупност свих потенцијала (кадровских, материјалних, организационих, нормативних и других) који се ангажују ради ове врсте заштите добара.

Када је у питању ниво националне безбедности, Водич кроз информациону безбедност у Републици Србији[205], наводи да Србији недостаје свеобухватна национална *стратегија развоја информационе безбедности* (донета је после писања ове студије, наша је примдба)[206] која би, налик стратегији ЕУ, представљала основу за успостављање целокупног нормативно-оперативног окружења. Стратегија би требало да дефинише кључне правце и циљеве деловања у области информационе безбедности, као и да препозна значај вишепартнерског модела и јавно-приватног партнерства итд. У погледу оперативних механизама, Србија има Одељење за борбу против високо-технолошког криминала (ВТК) при МУП-у, као и посебно Одељење Вишег јавног тужилаштва у Београду за територију Србије, док је на нивоу судства дефинисана специјална надлежност за ВТК и то кроз посебно одељење при Вишем суду у првом степену, односно Апелационог суда у другом степену. Закон о информационој безбедности[207] такође предвиђа оснивање Националног центра за превенцију безбедносних ризика у ИКТ системима (енгл: *Computer Emergency Response Team – CERT*), смештеног при Регулаторној агенцији за електронске комуникације и поштанске услуге (РАТЕЛ).[208]

Одељење за борбу против високо-технолошког криминала (ВТК), организационо се налази у оквиру Службе за борбу против организованог криминала, Управа криминалистичке полиције, Дирекција Полиције, Министарства унутрашњих послова, (Схема број 8: *Организациона позиција Одељења за високотехнолошки криминал у Управи криминалистичке полиције*).[209]

Посебно одељење за високотехнолошки криминал организовано је у оквиру Вишег јавног тужилаштва у Београду и поступа ради откривања, кривичног гоњења и суђења учиниоцима кривичних дела код којих се као објекат или средство извршења кривичних

[205] *Водич кроз информациону безбедност у Републици Србији*, Центар за евроатланске студије – ЦЕАС и Мисија ОЕБС у Србији, Београд, 2016. година, доступно на: https://www.osce.org/sr/serbia/272206?download=true

[206] *Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. Године*, "Службени гласник РС", број 53 од 30. маја 2017. године, доступно на: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/53/1/reg

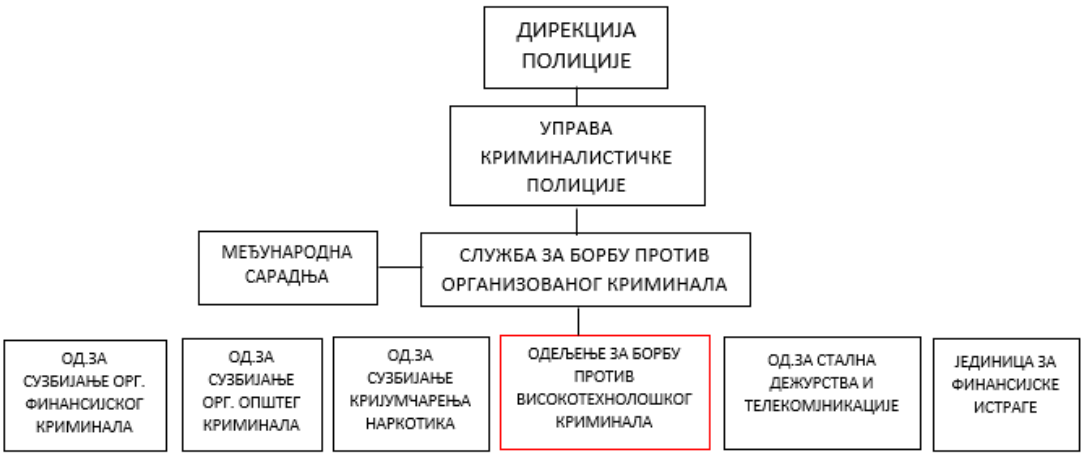
[207] *Закон о информационој безбедности*, „Службени гласник РС", бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019. године, доступно на: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg

[208] *Ibid*, стр. 13.

[209] Доступно на: http://arhiva.mup.gov.rs/cms_lat/UKP.nsf/sbpok.h?OpenPage

дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.[210]

Схема број 8: ***Организациона позиција Одељења за високотехнолошки криминал у Управи криминалистичке полиције***



Национални центар за превенцију безбедносних ризика у ИКТ систему Републике Србије (ЦЕРТ), основан је у оквиру Регулаторне агенције за телекомуникације и поштанске услуге, у складу са Законом о информационој безбедности. Примарна задужења Националног ЦЕРТ-а су координација превенције и заштите од безбедносних ризка у информационо-комуникацијским системима (ИКТ системима) на националном нивоу. Национални ЦЕРТ прикупља и размењује информације о могућим ризицима, а затим обавештава, упозорава и саветује лица која управљају ИКТ системима, као и јавност Републике Србије.[211]

Влада Републике Србије донела *Акциони план за 2018. и 2019. годину*, за спровођење Стратегије развоја информационе безбедности.[212] У овом документу је дат преглед планираних активности, а један од учесника активности је Народна банка Србије, чије смо учешће, полазећи од предмета истраживања, посебно приказали (Табела број 3: *Активности Народне банке Србије према Акционом плану за 2018. и 2019. годину*).

Добар пример мера које се могу донети на националном нивоу за заштиту информација у банкама и финансијским институцијама су *Препоруке које је дала НБС у вези са Corona*

[210] *Информатот о раду Вишег јавног тужилаштва у Београду*, доступно на: https://bg.vi.jt.rs/informator/
[211] Доступно на: https://www.ratel.rs/cyr/page/cyr-nacionalni-cert

[212] *Акциони план за 2018. и 2019. годину, за спровођење Стратегије развоја информационе безбедности*, Закључак са седнице Владе, 91. седница Владе Републике Србије, 28. август 2018. године, доступно на: https://www.srbija.gov.rs/prikaz/329365

кризом, у циљу подизања свести банака и финансијских институција о повећаном ризику и мерама које треба предузети.[213]

Табела број 3: ***Активности Народне банке Србије према Акционом плану за 2018. и 2019. годину***

ОПИС АКТИВНОСТИ	ИНДИКАТОР	УЧЕСТВУЈУ
1.1.1. Унапређење кадровских, стручних, техничких и организационих капацитета надлежних институција за размену података о инцидентима и реаговање на инциденте	Запошљавање стручних кадрова и подизање организационих капацитета надлежних институција у области информационе безбедности (5 запослених).	МТТ РАТЕЛ **НБС** ИТЕ МУП ВБА
1.1.3. Успостављање апликације за размену информација, као и сарадња у случају инцидената који значајно угрожавају информациону безбедност између Надлежног органа, Националног ЦЕРТ-а, ЦЕРТ-а републичких органа, Посебних ЦЕРТ-ова у Републици Србији и других државних и приватних субјеката	Успостављена апликација и механизам размена информација о инцидентима	МТТ РАТЕЛ **НБС** ИТЕ МУП
1.1.5. Дефинисање критеријума за класификацију инцидената у ИКТ системима од посебног значаја	Дефинисани критеријуми на основу којих се одређује степен озбиљности инцидента у ИКТ системима од посебног значаја	МТТ РАТЕЛ МУП ВБА ИТЕ **НБС**
1.1.6. Спровођење обука за запослене у надлежним органима о	Број запослених у надлежним органима који су прошли обуку	МТТ РАТЕЛ

[213] *Препоруке за безбедност IS CORONA Awarness*, Центар за супервизију информационих система, НБС, 23. март 2020. године, доступно на: https://www.nbs.rs/internet/cirilica/scripts/showContent.html?id=15338&konverzija=no

поступању у случају инцидената у ИКТ системима	(15 запослених годишње)	**НБС** ИТЕ АМРЕС

У прегледу смо дали субјекте који учествују у реализацији планираних активности Акционим планом, где је учешће НБС истакнуто болдованим фонтом. За потребе нашег рада, и да би стекли утисак о комплексности Стратегије, у легенди смо навели све субјекте који учествују у реализацији, где су они који су у нашој табели обележени тамнијим фонтом.

АМРЕС	**АКАДЕМСКА МРЕЖА РЕПУБЛИКЕ СРБИЈЕ**
БИА	БЕЗБЕДНОСНО ИНФОРМАТИВНА АГЕНЦИЈА
ВБА	**ВОЈНОБЕЗБЕДНОСНА АГЕНЦИЈА**
ВОА	ВОЈНООБАВЕШТАЈНА АГЕНЦИЈА
ИТЕ	**КАНЦЕЛАРИЈА ЗА ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ И ЕЛЕКТРОНСКУ УПРАВУ**
КСЗНБТП	КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА
МЗ	МИНИСТАРСТВО ЗДРАВЉА
МО	МИНИСТАРСТВО ОДБРАНЕ
МП	МИНИСТАРСТВО ПРАВДЕ
МПНТР	МИНИСТАРСТВО ПРОСВЕТЕ, НАУКЕ И ТЕХНОЛОШКОГ РАЗВОЈА
МРЗБСП	МИНИСТАРСТВО ЗА РАД, ЗАПОШЉАВАЊЕ, БОРАЧКА И СОЦИЈАЛНА ПИТАЊА
МСП	МИНИСТАРСТВО СПОЉНИХ ПОСЛОВА
МТТТ	**МИНИСТАРСТВО ТРГОВИНЕ, ТУРИЗМА И ТЕЛЕКОМУНИКАЦИЈА**
МУП	**МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА**
НБС	**НАРОДНА БАНКА СРБИЈЕ**
РАТЕЛ	**РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ**
РЈТ	РЕПУБЛИЧКО ЈАВНО ТУЖИЛАШТВО
УНИ	УНИВЕРЗИТЕТИ
ЦЕРТ	ЦЕНТАР ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА

Наше је мишљење, да и примена међународних стандарда и примера најбоље праксе може да буде део стратегије мера у заштити информација, што зависи од контекста у којем се ови документи примењују у оквиру организације (посматрано од нивоа привредних организација до државног и међудржавног нивоа). За потребе нашег рада, ми ћемо овај аспект детаљније приказати у поглављу о нормативној уређености заптите информација.

2. Организационо уређење заштите информација

Приликом разматрања мера заштите, навели смо тумачење Петровића, који наводи да су мере заштите одговор на питање „чиме“ штитити, што подразумева идентификацију свих мера које стоје на располагању у изградњи целовитог и поузданог ситема заштите.[214]

Полазећи од нашег предмета истраживања, сматрамо да је корисно да прикажемо начин на који аутор разврстава мере заштите, будући да су према његовом мишљењу мере организационог уређења заштите информација, заједно са правним и кадровским, налазе у области нормативног уређења области (Табела број 4: *Врста мера заштите информационе безбедности*).

Ми смо мишљења да научна класификација свакако доприноси бољем разумевању проблема истраживања, али је за наше истраживање приоритет одређивање садржаја организационог и нормативног уређења заштите информација, одакле нећемо давати посебан коментар на овакву поделу предметних активности, већ истичемо значај којим она доприноси одређивању садржаја феномена који истражујемо. У том смислу ближи смо становишту да све набројане мере не треба посматрати као коначну и затворено листу активности, већ их треба равноправно третирати као посебне области у остваривању заштите информација (нормативне, организацоне, логичке итд.).

Све ове мере могу се разврстати у различите логичке целине, у зависности од потреба конкретног система. Мишљења смо да организационо и нормативно уређење заштите информација, у том смислу, могу као активности представљати константу, односно мишљења смо да су увек присутне, без обзира на различите потребе организација (различите и по врсти делатноси и по њиховој величини).

Начин уређења организационе структуре је одређен са више елемената, као што су:

- организациона култура;
- величина организације;
- буџет за потребе безбедности.

[214] Петровић, С., *op.cit*, стр. 21

Табела број 4: ***Врста мера заштите информационе безбедности***[215]

ОПИС МЕРА		
ВРСТА МЕРА ЗАШТИТЕ	**ПОДГРУПА АКТИВНОСТИ**	**УЖА ОБЛАСТ**
НОРМАТИВНЕ	*ПРАВНЕ*	– Стварање јединствених основа заштите
		– Заштита приватности
		– Заштита интелектуалне својине
		– Санкциониање злоупотребе информатичких средстава
	ОРГАНИЗАЦИОНЕ	– Организациону структуру и систематиизацију
		– Дефинисање радног процеса
		– Развој софтверских система
		– Документацију
		– Стандарде
		– Планирање
		– Права и одговорности
		– Рестриктивне мере
		– Рад ван радног времена
		– Поверљивост
		– Надзор и контролу
		– Упозорења
		– Санкције
	КАДРОВСКЕ	– Планирање кадрова
		– Избор кадрова
		– Распоређивање кадрова
		– Руковођење
		– Мовивацију и лојалност кадрова
		– Стручно усавршавање и безбедносно образовање
		– Унапређивање и награђивање
		– Мађуљудске односе
		– Политику годишњих одмора
		– Прекид радног односа
ФИЗИЧКО-ТЕХНИЧКЕ		– Физичко-техничко обезбеђење
		– Електронско обезбеђење
		– Заштиту од електро магнетног зрачења
		– Заштиту од пожара
		– Против поплавну заштиту
ЛОГИЧКЕ		– Приступним путевима систему
		– Приступу ресурсима који се штите
		– Начином коришћења ресурса

Ми смо мишљења да је *организациона култура* у том смислу најважнији елемент, будући да уколико виши менаџмент и остали запослени не сматрају да је заштита информација битна за остварење циљева организације, онда ће се напори које чини (ма како они били велики и на професионално високом нивоу) информациона безбедност у пракси остваривати са скромним резултатима, а сама организација ће ове напоре сматрати супротним својим интересима и узалудним трошењем ресурса. Више научних радова које смо приказали у поглављу о прегледу референтних радова који се односе на наш предмет истраживања, подржавају ову тезу.

Величина организације и доступни ресурси директно се одражавају на структуру ресурса за заштиту информација. Када су у питању субјекти са великим и захтевним *IT* системима, она се очеује већа подршка (улога) од стране информационе безбедности. Велики системи могу чак имати посебне секторе (енгл: *divisions*) који су посвећени пословима информационе безбедности, укључујући и функцију *CISO (*енгл: *chief information security officer − CISO),* односно особе које представљају извршни виши нивоу у организацији, која је одговорна за заштиту информација, као и за те сврхе посвећене менаџере (безбедности),

[215] Извор: предавање Петровић, С.: *Заштита информација*, Удружење *IT* вештак, 17. септембар 2014. године, Београд

администраторе и друго техничко особље. Мање организације, са друге стране, могу имати само једног администратора безбедности.

Износ буџета за информациону безбедност је у директној повезаности са величином организације. У пракси, не постоји прави стандард за величину буџета за информацијску безбедност. Ове величине могу бити исказане различито, као однос буџета за заштиту информација према оствареном приходу организације, или као однос броја запослених у информационој безбедности према укупном броју запослених у организацији, односно на неки други начин.

Витман и Маторд, дали су преглед основних функција које треба да буду укључене у програм заштите информација. Ови аутори кажу да те функције нису обавезујуће да буду развијене у оквиру Одељења за информациону безбедност, али да свакако треба да буду развијене „негде у организацији“ (Табела број 5: *Потребне функције за организовање програма заштите информација*).[216]

Табела број 5: Потребне функције за организовање програма заштите информација

ФУНКЦИЈА	ОПИС	НАПОМЕНА
Процена ризика (*Risk Assessment*)	Процењује присутан ризик у *IT*-у	Идентификује изворе ризика и предлаже мере за њихово смањење
Управљање ризиком *Risk management*	Спровођење контрола у циљу смањења ризика	Обично се обавља заједно са *Risk Assessment*-ом
Тестирања *(Systems Testing)*	Оцењује рањивост постојећих софтвера и проверава да ли су нови програми усклађени са усвојеним безбедносним политикама	Обично је део *Incident response and/or risk management functions*
Креирање политика (Policy)	Осмишљавање и промоција одговарајућих правила	Мора бити усаглашено са доношењем правила у другим областима у оквиру организације
Законитост *(Legal Assessment)*	Усклађенот са законима и другим прописима	Готово увек је ван Одељења за *IS/* или *IT*
Одговор на инциденте *(Incident Response)*	Пружање најранијег одговора на све врсте инцидената и умањење њихових негативних ефеката	Мора да укључи средњи менаџмент из других пословних функција, како би било

[216] Прирећено према: Whitman, M., Mattord, H. J., *op.cit*., стр. 161-162

		омогућено управљање у инцидентима
Планирање *(Planning)*	Истраживање и стварање планова у области безбедности информација. Често учествовање у пројектима који су стратешки за целу организацију	Мора координарати са другим процесима и политикама у организацији
Мерење *(Measurement)*	Користећи постојећи систем кононтроле мерити све аспекте информационе безбедности	Потребне су благовремене и тачне статистике да би се доносиле исправне одлуке
Усаглашеност *(Compliance)*	Проверава да ли систем и *network* администратори поправљају уочене слабости брзо и правилно	Представља изазов за кориснички сервис јер је тешко бити истовремено фокусиран на клијенте и испуњавати ове обавезе у исто време
(Centralized Authentication)	Управљање мрежним и системским акредитацијама за целу организацију	Обично се делегира у *help desk* или сличну функцију
Администрација *(Systems Security Administration)*	Администрирање и конфигурација рачунара	Многе организације управо овде делегирају функције заштите информација, што (наравно) може да преставља конфликт за спровођење безбедносних програма
Обуке *(Training)*	Обучавање свих запослених за заштиту информација. *IT* обучавати за посебне техничке методе, поред општих тема за *IS*	Неке од ових обука могу да се реализују у сарадњи са организационим делом који иначе води рачуна о обукама
Мрежна безбедност *(Network Security Administration)*	Адмионистрирање мреже	Многе организације управо овде делегирају функције заштите информација, што (наравно) може да преставља конфликт за спровођење безбедносних програма
Процена рањивости *(Vulnerability Assessment)*	Лоцира рањивости информационих ресурса	Некада се назива и *penetraton testing* и обично је *outsorcing*-овано

Примећујемо да се на овакав начин изложена функционалност послова заштите информација своди на проблематику која је у најужој вези са *IT* ресурсима, одакле изостаје поглед који ми преферирамо у овом истраживању, а то је да послове заштите информација сагледамо у ширем контексту, а пре свега са аспекта организационих и нормативних мера.

Витман и Маторд[217] наводе да организације са више од хиљаду радних станица вероватно имају сопствене запослене, који ће им омогућити да испуне већину функција наведених у претходној табали коју смо дали. Овакве организације често организују посебне организационе целине. Како су и саме организације увек различите по својој организационој структури, тако је и организовање безбедносних функција прати ове специфичности конкретних организација. Одељења за информациону безбедност у великим организацијама имају тенденцију да формирају и преобликују унутрашње групе, како би обезбедиле функционисање већине функција заштите информација. Аутори наводе да се функције заштите информација обично деле у групе у великим организацијама, а да се у мањим ствара и мањи број група, али тако да увек постоји организациони део за заштиту информација. Један од могућих приступа је одвајање функција заштите информација у четити групе, и то:

1. функције које обављају нетехничке пословне јединице изван IT-а, као што су правни послови или тренинг;

2. функције које обављају IT групе изван подручја информационе безбедности, као што су:
   - послови администрације система безбедности (енгл: *sistem security administration*);
   - администрација мрежне безбедности (енгл: *network security administration*);
   - централизована администрација безбедности (енгл: *centralized security administration*).

3. функције које се обављају у одељењу за информациону безбедност, као што су:
   - процена ризика (енгл: *risk assessment*);
   - тестирање система (енгл:*system testing*);
   - одговор на инцидент (енгл: *incident response*);
   - планирање (енгл:*planning*);
   - мерење (енгл: *measurement*);
   - процена рањивости (енгл: *vulnerability assessment*).

4. функције које се обављају у одељењу за информациону безбедност, а произилазе из законских обавеза, као што су:
   - писање безбедносних политика (енгл: *pollicy*);
   - Усклађеност са законом/ревизија (енгл: *compliance/audit*);
   - Управљање ризиком (енгл: *risk management*).

Дужност руководиоца информационе безбедности (енгл: *chief information security officer – CISO*) је да организује примену функција безбедности информација „негде“ у организацији. Велике организације обично имају сопствене кадрове за остваривање програма заштите информација. Колика ће бити организациона структура зависи од низа фактора, укључујући

[217] *Ibid,* 163. – 167.

потребе које следе из осетљивости доступних информација, законских прописа који важе за конкретну индустрију (као што је у банкама и финансијским институцијама), као и од профитабилности организације. Што су веће финансијске могућности организације за одвајање буџета за потребе заштите информација, то ће пре имати већу организацијску структуру за заштиту информација. Аутори наводе да типично велика организација обично има преко двадесет администратора/техничара (којом приликом у тај број рачунају и стално запослене и оне са непуним радним временом) који су посвећени пословима заштите информација. Како смо претходно навели, поједине послове (функције) заштите информација могу да обављају и запослени који приоритетно имају друга пословна задужења, а пример су IT администратори који су задужени за функционисање појединих сервера од чије функционалности зависи пословање целе организације, па они том приликом одржавају и безбедносне апликације које се налазе на њему. Јако велике организације могу имати и преко двадесет стално запослених на пословима заштите информација, као и преко четрдесет запослених који су уз своје редовне обавезе ангажовани на испуњавању дела обавеза у информационој безбености.

Организације са средњом величином, оне које имају од сто до хиљаду радних станица, још увек су довољно велике да могу да примене вишеслојни приступ безбедности који смо видели код великих организација, али са мање наменских група и више додељених функција у оквиру сваке групе. Посебно, овде се многе безбедносне функције додељују IT-у. Проблем који се јавља је појава тенденције да се игноришу неке од функција које смо навели у прегледу функција које су потребне за организовање програма заштите информација, а посебно када одељење за информациону безбедност (енгл: *information security department – IS department*) не може да постигне да обавља поједине активности, а IT односно друго одељење није охрабрено да ту функцију обавља уместо њега. У том случају руководилац безбедности мора да побољша сарадњу између ових група и мора да представља лидера који је свестан ограничености перформанси организације.

Полазећи од предмета истраживања нашег рада, нећемо посебно разматрати организацију заштите информација у малим организацијама, које имају мање од сто радних станица. Ипак, напоменућемо да су овде безбедносне функције сведене на минимум и да се оне које постоје, обављају у различитим организационим деловима, У оваквим организацијама често се ангажују спољашњи сарадници, за питања које овакве организације не могу саме да реше, а локални администратори иформационог система обављају придружено послове за које имају потребна знања. Мале организације углавном имају потребне политике за заштиту информација, а спољни сарадници своје активности обављају преко веба. Предност оваквих организација у односу на веће је у томе што се тренинг за повећање безбедносне свести у погледу заштите информација може да спроводи појединачно, а запосленима је увек на располагању IT аминистратор за пружање одговарајућих одговора и помоћ. Такође, велика предност је број запослених, где се они практично познају између себе, одакле се лакше успоставња одговарајућа безбедносна култура организације.

3. Место информационе безбедности у организацији

У великим организацијама одељење за информациону безбедност често се налази у оквиру IT-а. Радом одељења руководи руководилац за информациону безбедност, који рапортира извршном директору задуженом за IT. Таква организација подразумева да су циљеви ова два руководиоца усаглашени, што у пракси зна да представља проблем. Са једне стране руководилац IT-а је задужен за ефикасност информационог система, а свако ограничавање приступа или успоравање процеса га ограничава да буде успешан у обављању ове функције. Руководилац безбедности је често у улози ревизора, јер се бави откривањем недостатака у информационој технологији, софтверу и активностима и процесима запослених, што некада може да омета обраду и приступ информацијама. Из ових разлога није тешко разумети потребу одвајања ових пословних функција (у основи је то избегавање сукоба интереса које може да има IT).

Истражујући питање о месту информационе безбедности (енгл: *information security – IS)* у организацији, са аспекта односа између информационе безбедности (IS) и IT-а, пронашли смо много текстова који говоре о овом питању. У најкраћем, данас стручњаци и научници препознају потребу раздвајања, у организационом смислу, ове две функције организација, али истовремено и примећују да се та трансформација одвија споро, али да ће дигитализација донети убрзавање овог процеса. Једна од тих студија показује податак да око 60% CISO (руководилаца информационе безбедности) рапортира CIO (енгл: *Chief information officer – CIO*), а да додатних 10% рапортира техничком директору (енгл: *Chief technology officer – CTO*), али да је у банкама та структура повољнија, будући да постоји регулаторни механизам у многим државама, због чега фукција безбедности информација рапортира пословној функцији која се бави ризиком, односно генералном директору (енгл: *Chief executive officer – CEO*). У истом тексту се наводи да је у Европској унији овакав тренд већ на снази, захваљујући доношењу и примени новог правног оквира (у примени је од 25. маја 2018. године), који прописује начин коришћења података о личности грађана Европске уније (енгл: *General Data Protection Regulation – GDPR*), о чему ће у нашем раду бити посебно речи у оквиру разматрања нормативног оквира уређења послова заштите информација.[218]

У многим случајевима, организационе део који је задужен за безбедност информација убачен је у структуру организације тако да показује њен маргинални статус. Организације које трагају за рационалним компромисом покушаће да пронађу такво место у организацији које ће омогућити баланс између потреба информационе безбедности и могућности организације. Идеална је позиција која ће да омогући да информациона безбедност постане део организационе културе, са напоменом да се подразумева да само позиционирање у

[218] Чланак: "Зашто се враћа расправа о улози руководиоца информационе безбедности и његовом месту у организацији", *Changing CISO's Reporting Structure: Why The Debate Is Back?*
Доступно на: https://www.cioandleader.com/article/2019/07/03/changing-cisos-reporting-structure-why-debate-back

организационој структури није и гарант да ће послови заштите информација бити оптимално организовани.

У даљем раду, даћемо преглед неких од могућих решења, како су то дали Витман и Маторд[219]

3.1. Информациона безбедност у оквиру *IT* послова

Ово је можда и најчешћа опција у пракси, а аутори тврде да се можда и 50% организација опредељаује за овакав концепт.[220]

Одељење за информациону безбедност организационо се налази у оквиру IT-а, а још једну линију рапортирања има према Одбору за безбедност. Као и свако решење, тако и овде можемо приметити предности и мане овакве организације.

Предност је што је олакшана комуникација са IT-ем, јер један менаџер одговара за организацију рада и руковођење обе пословоне функције, па је тиме олакшана координација рада и брже решавање оперативних питања.

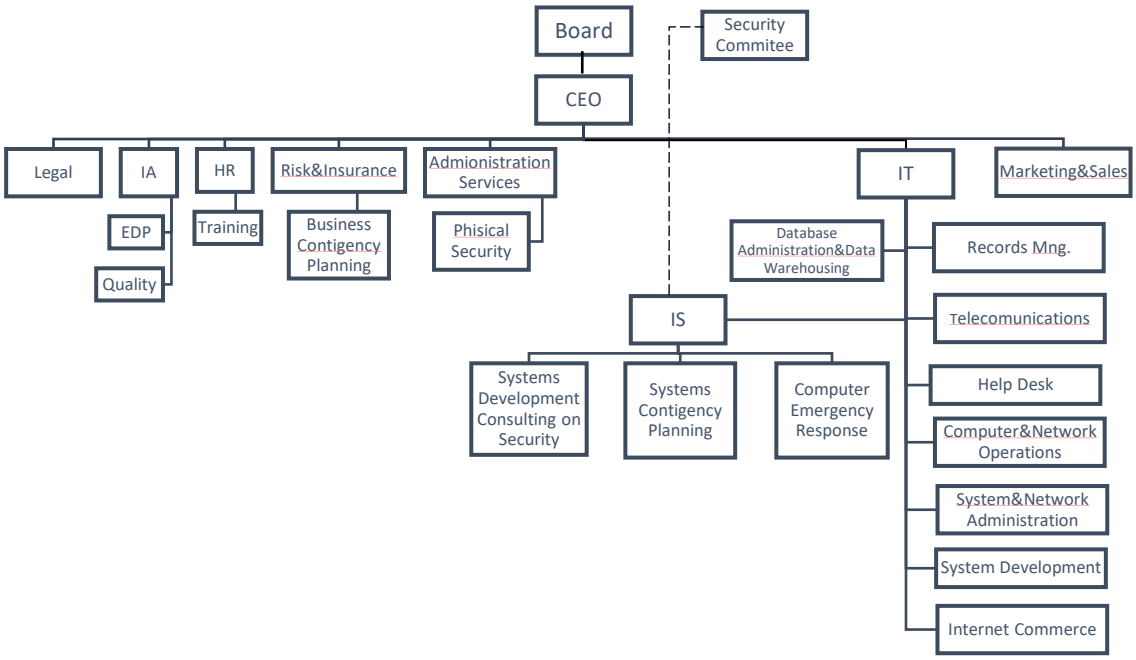
Недостатак овакве организације је у могућности сукоба интереса руководиоца IT-а, будући да руководилац заштите информација може да има, а што и јесте за очекивати, професионална неслагања за надређеним руководиоцем. Раније смо изнели у тексту, да је таква природа послова, да се од IT-а очекује брзо и ефикасно решавање радних задатака – што је очекивајуће, полазећи од чињенице да целокупно пословање зависи од функционалности IT-а. Са друге стране, природа послова информационе заштите јесте таква да често захтева анализе и да трага за логичним одговорима и тако тражи пропусте у организацији. Оно што за IT мора да се обави сада и одмах, за *IS* (безбедност или заштита информација, енгл: *Information Security* – IS) не само да не мора да значи, већ је и очекивајуће да приоритет буде аналитичност и сагледавање могућих ризика неке операције.

Информациона безбедност не сме да прави компромисе, већ потенцијалне претње мора да сагледа и да у зависности од ризика одмах обавести највише органе управљања. Чини се да оваква пракса, у условима ове организације рада, није реална у стварности. Не због недовољно стручног знања ангажованих стручњака, већ због природе људског понашања, где није за очекивати да у организацији све добро функционише у условима сталне професионалне конфронтације. Банализовано, оно што за информациону безбедност може да буде приоритет, то не мора да буде тако из перспективе IT-а – и обрнуто.

Ова могућа, а ми би рекли и очекивајућа, некомпатибилност две важне пословне функције у организацији су још један мотив да се проблему организације информационе безбедности приступи тако да се њена улога у организацији, односно у целокупном систему заштите не посматра изоловано, већ у склопу комплетне безбедносне функције организације.

[219] Whitman, M., Mattord, H. J., *op.cit.*, стр. 172. - 182.
[220] *Ibid*

Схема број 9: ***Информациона безбедност у Одељењу IT-а***



Даље, ако посматрамо организациону културу, дакле вредности и ставове које дели (компактна) група, а у овом случају овде јесте реч о групи у оквиру једног организационог дела, онда је за очекивати да приступ према информационој безбедности буде у складу са стручном области која их повезује, а то је у овом случају (и увек када је IT у питању) технички приступ.

У оваквим организацијама ће се најчешће информациона безбедност, у неформалном жаргону сасвим извесно, називати сајбер или IT безбедност, а такав приступ претходно смо критиковали као ненаучан и нефункционалан, са аспекта постизања жељеног стања безбедности организације.

Још један аргумент за забринутост и у вези са претходно наведеним, јесте чињеница да се организационе део физичке безбедности налази раздвојен од информационе безбедности, чиме може да се програмира да ове две фукције безбедности буду суштински, а не само формално раздвојене, са различитим политикама пословних функција којима припадају, а тиме и различитим приступ остваривању безбедности организације.

Поред могућег конфликта интереса заштите информација и IT безбедности, при чему се не сме занемарити чињеница да се увек у IT-у обавља и технички део заштите информација (администрирање, доделе привилегија корисницима информационог система, контроле, техничке мере заштите ИКТ система и друго), на нивоу исте пословне функције, може се поставити питање квалитетног извештавања Одбора за безбедност.

Одбор за безбедност је, како ћемо видети и у свим другим предлозима организовања заштите информација, стално присутан орган у свим моделима могуће организације, јер је реч о телу где је потребно да се сусрећу све информације из пословања које могу да имају последице на њену безбедност. Истовремено, ово је место где све пословне функције треба да добију квалитетне информације које се односе на могуће претње за пословање организације. Реч је дакле о двосмерном процесу, где безбедносна фунцкија треба да доставља извештаје о безбедности организације и да се информише о безбедносном аспекту пословања који се одвија у свим другим пословним функцијама. Из тих разлога Одбор за безбеност чини највиши менаџмент пословних функција које организација процени да су критичне, у случају већих организација, а када су у питању оне средње и мале величине, онда и сви представници пословних функција пратећи организациону поставку. Одбор за безбедност је по својој позицији у организацији задужен и за учестовање у дефинисању безбедносне политике организације, и за разматрање других важних питања која се односе на безбедносну проблематику.

Ако сагледамо овај опис надлежности које обавља Одбор за безбедност, онда је видљиво из којих разлога је он витално заинтересован да добија квалитетне информације о стране стручних служби које се баве пословима безбедности. Из разлога сукоба интереса који смо описали да се догађа у оваквим организацијама, а који потиче из IT-а, јер се у њему налази и Заштита информација, као и због раздвојености система безбедности на више пословних функција, у овом случају на IT и Опште послове, може се изразити бојазан да ли ће Одбор за безбедност добијати потребне информације.

Може деловати као логична аргументација да се послови безбедности информација пројектују у IT пословну функцију, са позиције ефикасности и ефективности, јер је IT место где се подаци и информације прикупљају, чувају и дистрибуирају заинтересованим корисницима, одакле би се могло помислити да је ово природно место где ће се послови заштите информација обављати најцелисходније. Ипак, наше је мишљење, да такав приступ занемарује шири контекст послова безбедности и правила која се односе на организационо понашање и саму природу понашања људи. У том смислу, увек је најбоље приликом пројектовања организације поставити питање – ко контролише контролоре.

3.2. Информациона безбедност у оквиру безбедносне пословне фукције

Претходно смо изнели особине сврставања послова заштите информација у групу послова заједно са IT-ем, где смо приметили да је, поред неких предности, један од недостатака разбијеност безбедносне функције организације на више пословних функција.

Посметрани приступ, где је већи број послова смештен у једну организациону целину, дакле превазилази функционалну подељеност, карактеришу ефикасније управљање и контрола у обављању послова безбедности у организацији.

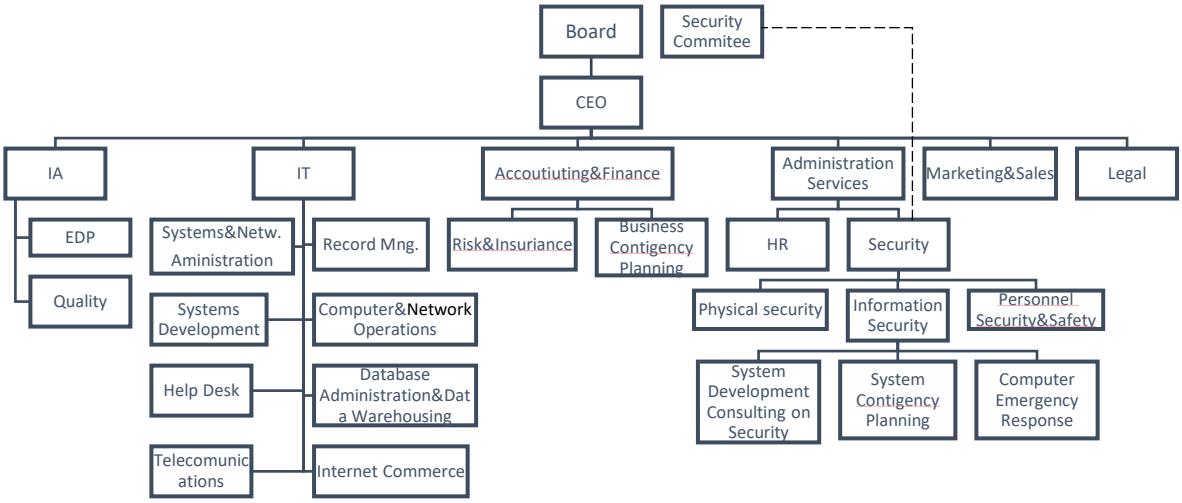
Поред послова заштите информација, у организацији се, према мишљењу аутора, обављају и следећи послови:[221]

- безбедност запослених;
- заштита од пожара;
- безбедност и здравље на раду;
- физичка безбедност.

У односу на претходни пословни модел, предност овакве организације је што шири област заштите и повећава ефикасност организације у остваривању своје безбедности.

Значај безбедност запослених (енгл: *Personnel Security*) проистиче из значаја које људи имају за фукционисање организације и постизање пословних циљева. Они у том смислу представљају и вредност компаније, а истовремено могу да буду и извор угрожавања. Исто тако, они могу да буду и предмет неког напада.

Схема број 10: ***Информациона безбедност у Одељењу за безбедност***



У раду који разматра питања идентификације претњи за безбедност организације које долазе од стране запослених, или где су запослени циљ напада, направљен је преглед извора ових претњи, које смо приказали у посебном прегледу (Табела број 6: *Преглед штета и последица које људи могу да нанесу организацији*).[222]

[221] *Ibid*

[222] Lobova, S.V, Bogovitz, A. V.: *The Subject-Object Identification of Personnel Security Threats*, Espacios, VOL 39 (Num. 24), 2018., доступно на: https://www.revistaespacios.com/a18v39n24/a18v39n24p34.pdf

Мишљења смо да преглед не обухвата све врсте догађаја, али примећујемо да се на овом примеру може показати колико је важно за организације да приликом организовања послова безбедности имају у виду предности повезаности различитих функција безбедности, и да је потребно да настоје да их окупе у оквиру једне пословне фукције – као што је у организационом примеру који посматрамо. Иако је у овом примеру реч о различитој групи послова у оквиру безбедности, (енгл: *Personnel Security*), налазимо неколико прожимања, пре него додирних тачака, са пословима информационе безбедности. То се односи на догађаје крађе интелектуалне својине, откривања поверљивих информација, уништења или оштећења докумената и друго.

Табела број 6: ***Преглед штета и последица које људи могу да нанесу организацији***

ИМПЛИКАЦИЈЕ	Штетна актиност долази од:		
	ЗАПОСЛЕНОГ	БИВШЕГ ЗАПОСЛЕНОГ	КАНДИДАТА ЗА ПОСАО
УНИШТЕЊЕ	Финансијске преваре, проневере, крађа интелектуалне својине или намерно оштећење имовине	Уништење важних докумената, оштећене имовине	
НЕФУНКЦИОНАЛНОСТ	Неодговорност и непажња, злоупотреба службених овлашћења ради стицања користи	Покретање судских поступака против послодавца	Употреба поверљивих информација у незаконите сврхе
УГРОЖАВАЊЕ	Откривање поверљивих информанција, њихово фалсификовање или уништење	Прослеђивање поверљивих информација конкуренцији или ширење лоших вести о послодавцу	Преношење информација конкуренцији или агнцијама за тражење кадрова

Ово је још један прилог објашњењу због чега је исправнији приступ да се у остваривању заштите информација посматрају и дигитална и аналогна област, а не само дигитална, као што је реч у „сајбер“ или „*IT*“ разумевању заштите информација, што смо разматрали на почетку овог поглавља – будући да интелектуална својина није, и не мора бити само у области ИКТ безбедости, што се односи и на документацију и иначе на информације, које могу бити један од објеката злоупотреба које чине људи у организацији, а од чега се организација штити и кроз *Personnel Security* пословну и безбедносну функцију.

Корист од успостављања функције „безбедности кадрова“, или „безбедности запослених“, видимо и на прегледу који су исти аутори дали када се посматрају запослени, не као извор (како они наводе „субјекат“ претњи) овога пута, већ као објекат претњи угрожавања безбедности организације, кроз неки облик имплементације пратњи, како наводе Лобова и

Боговиз (Табела број 7: *Преглед штета и последица којима могу да буду изложени запослени*).

Остале послови безбедности, који су у оваквој организацији у истој организационој јединици са пословима информационе безбедности, нећемо посебно разматрати, будући да за све њих важи да се у неком смислу у (обостраном) односу са заштитом информација, а за области заштите од пожара и безбедности и здравља на раду (у енглеском говорном подручју се обично називају групом *Safety* послова) постоји и законска обавеза уређености тих послова у организацији.

Што се тиче функционалности Одбора за безбедност, организација која сажима различите безбедносне функције на једном месту, као што је у овом примеру дато, има најмање исту ефикасност као претходни модел кад су послови информационе безбедности били у оквиру IT пословне функције. Чак, у сада посматраном моделу не постоји опасност сукоба интереса информационе безбедности са IT-ем, о чему смо говорили код модела „*IS* у *IT*-у".

Табела број 7: ***Преглед штета и последица којима могу да буду изложени запослени***

ИМПЛИКАЦИЈЕ	Штетна активности долази од:					
	СОЦИЈАЛНОГ ОКРУЖЕЊА	КРИМИНАЛАЦА	КОНКУРЕНЦИЈЕ	ДРУГИХ ЗАПОСЛЕНИХ	ПРИРОДЕ ИЛИ ДРУГЕ НЕСРЕЋЕ	ДРЖАВЕ
УНИШТЕЊЕ		Убиство, покушај убиства, отмица запосленог или његове породие		Анимирање за злоупотребу треће стране	Смрт запосленог	
НЕФУНКЦИОНАЛНОСТ		Саучесништво или охрабривање на крађу	Малверзација	Малверзација	Нарушавање и губљење здравља због непоштовања БЗР	Прикривање компромитујућих информација
УГРОЖАВАЊЕ	Оговарање, ширење измишљених вести			Психолошки терор, мобинг и друго нарушавање интегритета личности		Незапосленост на тржишту рада

Става смо да се груписање послова безбедности на једно место у организацији, посебно када су у питању оне велике, постижу многе предности у ефикасности система заштите, одакле смо склони да овакав модел називамо − холистичким приступом у организовању послова безбедности.

На крају, али не најмање важно, сматрамо да блискост безбедносе функције са било којом другом (не само са IT- ем, само што је тада проблем израженији) пословном функцијом, увек може довести до проблема сукоба интереса. То је због разлога који долазе из законитости понашања људи у организацији, а не неких других, јер како ће безбедносна функција да актуелизује постојеће претње и ризике, ако су ти пропусти последица одговорности менаџера који је формално задужен и за безбедност, поред његове „матичне“ пословне функције.

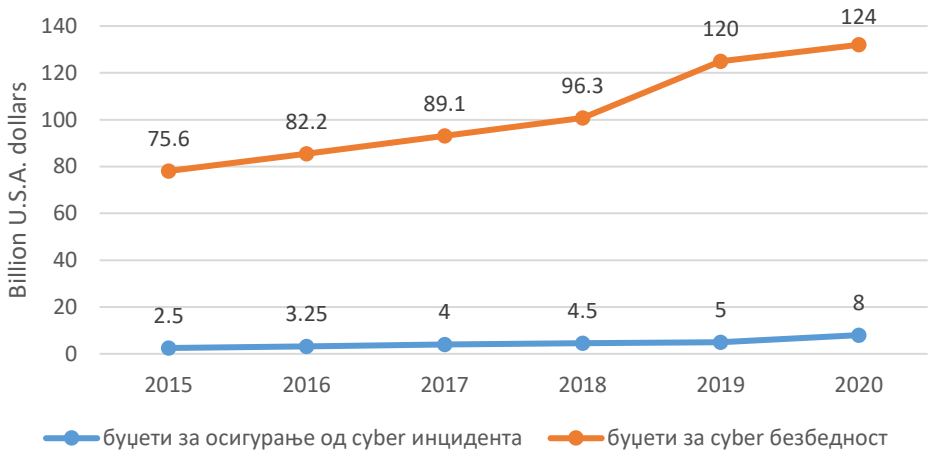
Идеалан модел, наше је мишљење, била би самостална пословна функција безбедности, са директном линијом рапортирања највишем менаџменту, односно власнику или његовом представнику.

Уважавајући претходно наведено, функционална блискост *HR*-а и послова безбедности може да покаже и одређене предности. Тај простор видимо пре свега у спровођењу обука за запослене за подизање безбедносне свести (енгл: *security awareness*), будући да је управо *HR* специјализован за организовање оваквих делатности у организацији (тренинга). Такође, од значаја је степен поверљивости приликом дељења информација, који се у компактним срединама лакше унапређује него у онима који то нису, а управо смо видели колики је простор у овој сарадњи када је у питању *Personnel Security*, будући да су онда на једном месту они који имају информације о кандидатима, бившиом сарадницима и запосленима (*HR)* и безбедносна пословна функција.

Питање буџетирања трошкова за безбедност је такође једно од кључних питања сваке организације. Опште је познато да се трошкови за „традиционалну безбедност“ у годишњим плановима рачунају као фиксни трошак, са сталном тенденцијом смањења, или благог повећања (услед фактора повећања других цена на тржишту). На другој страни, буџети за ИКТ су све већи, што је условљено како потребама унапређења технологије, тако и потребама заштите исте. Ово може бити, ако посматрамо површно, један од аргумената због чега је добро да се послови информационе безбедности смештају у оквиру IT пословне функције, јер ће руководиоци IS послова лакше доћи до средстава за своје пројекте (преко IT буџета).

Према подацима *Statiste,* буџети за потребе информационе безбедности у свету стално расту, а за ове потребе ће се, процена је, у 2020. години, потрошити преко сто двадесет милијарди долара (Графикон број 7: *Кретање буџета за cyber безбедност и осигурање од оваквих штета, на светском нивоу, у периоду од 2015. до 2020. године*).

Графикон број 7: ***Кретање буџета за cyber безбедност и осигурање од оваквих штета, на светском нивоу, у периоду од 2015. до 2020. године***[223]



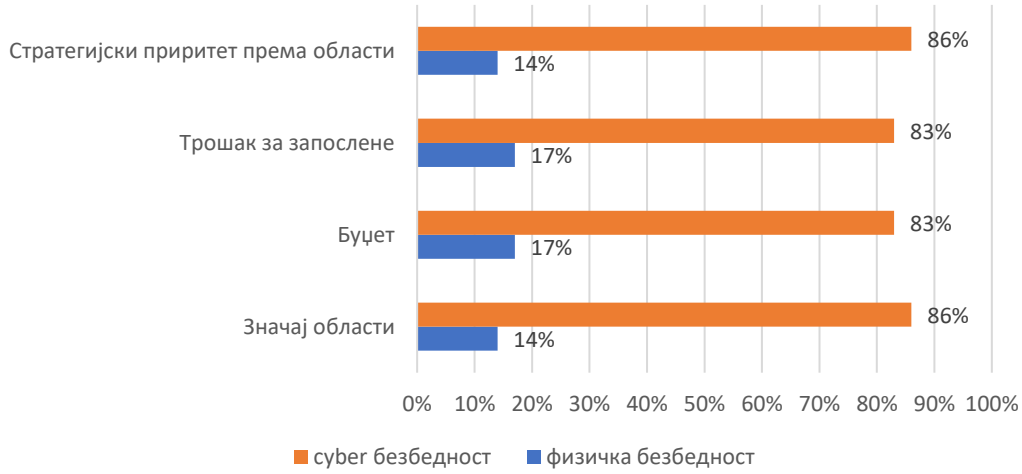
Напомињемо да су подаци дати за појам *cyber* безбедности, о чему смо на почетку овог поглавља приказали да данас углавном представља синоним за појам заштите информација. Такође, овом приликом напомињемо да је у прегледу дат податак за буџете који се односе за плаћање *полиса осигурања*, који се издваја за ублажавање евентуално насталих губитака од угрожавања информација, што се у котенксту нашег истраживања може посматрати као још једна *мера заштите информација*, а који према наведним подацима износи око 6.5 % годишњег буџета, на светском нивоу – податак који стоји као користан за стручњаке који се баве планирањем буџета за потребе заштите информација.

Односи буџета, за различите делове система безбедности је увек индикативан податак који може да нас упути у филозофију једне организације, у смислу разумевања менаџмента према безбедносним потребама, а што се увек, наше је мишљење, прелама и на органиизациони модел ових послова.

Према подацима *Loss Prevention Magazine*, извршни менаџмент данас има многоструку већу свест према значају информационе безбедности, у односу на физичку безбедност (Графикон број 8: *Перцепција менаџмента према значају области физичке и информационе безбедности*).

[223] *Annual cyber security and cyber insurance spending worldwide from 2015. to 2020., Statista*, 2020., доступно на: https://www.statista.com/statistics/387868/it-cyber-securiy-budget/

Графикон број 8: ***Перцепција менаџмента према значају области физичке и информационе безбедности***[224]



Изнети подаци нас наводе на закључак да су данас организације, услед последица које могу да настану угрожавањем информационих ресурса, склоне да послове информационе безбедности и послове физичке безбедности не посматрају заједно, већ да услед (несумњивог) значаја који има IS своју пажњу обраћају само на ове послове. Ову рефлексију можемо да приметимо и у организационим моделима које посматрамо.

У тексту се наводи и да руководиоци који су учествовали у анкети декларативно (ипак) разумеју да се сајбер безбендост не може посматрати одвојено од других функција безбедности, у овом случају од физичке безбедности.

Испитаници теже ка холистичком приступу, каже се у овом истраживању, јер су претње измешане и укључују претње од самих запослених. Један од закључака истраживања је да је потребан интегрисани приступ који захтева координацију и размену информација између физиче и информационе безбедности, као би се осигурало да се њихови програми допуњују, а не да ометају једни друге.

Аутори се позивају на налазе студије која је анализирала случај губитка дела IT опреме, где се у закључку наводи да је заштита мрежа и система постала тешка и да ће се тај тренд наставити (биће све теже) једнако као и развој технологије. Један од централних закључака, препорука руководиоцима заштите информација јесте да *морају да ближе сарађују са сегментом физичке безбедности у својим срединама, јер је потребно да се системи*

[224] Прирећено према: *Cyber Security vs. Physical Security: What Do CEOs Care About?*, Loss Prevention Magazine, 2018. Доступно на: https://losspreventionmedia.com/cyber-security-vs-physical-security-what-do-ceos-care-about/

заштите посматрају комплексно, и да је потребно организовати их тако, да структура безбедносног система подсећа на листова црног лука – дакле слојевито.[225]

Модел слојевите заштите (слично смо ми показали приказивањем модела слојевите заштите информација код Џигурског), упућује на закључак аутора да менаџмет компанија треба да разуме да је *безбедност процес, а не готов производ или један пројекат*.

Посматрано на нивоу организације, износи буџета ће се разликовати у зависности од тога где је функција безбедности организационо смештена. Они ће некада бити већи (када су у IT-у), а некада, у складу са степеном њихове маргинализације – мањи (последично и мање ефикасни за организацију).

Ако искључимо ове крајње случајеве, да је заштита информација смештена у IT-у, или да је скрајнута у неку другу пословну функцију где логички не припада, можемо да приметимо да варијације на тему где припада безбедност не стварају значајне разлике у буџету компаније. Они остају приближних вредности, али проблем видимо у томе што се сваки менаџер, у оквиру пословне функције за коју је задужен, бори за остваривање што бољих личних резултата (руководећи се формулом: што бољи резултати, уз што мање оптерећење трошкова организације), јер му на тај начин расте углед у средини где ради.

Ово је још једна додирна тачка организационог понашања и остваривања послова безбедности. Локалне политике у организацији (политике пословних функција) боре се за што боље интерно позиционирање у компанији, користећи при томе мерљивост према формули како смо навели.

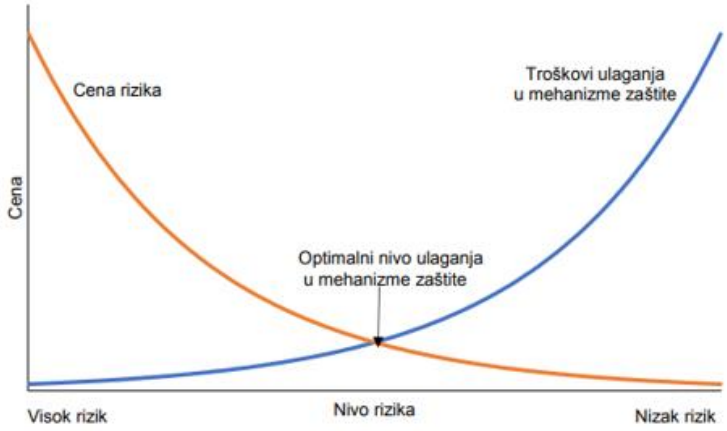
За безбедност – ефикасност је мерљива количином спречене штете за организацију, која долази из скупа свих претњи и преко рањивости се „наплаћује“ од организације. Колика штета је спречена, захваљујући свим безбедносним мерама, величина је до које је тешко доћи (Графикон број 9: *Однос улагања у механизме заштите и уштеде услед спречавања реализације напада*[226]). Да би овај податак био реалан, потребно би било установити регистар свих штетних догађаја који су се могли догодити компанији, а нису (и због чега нису, захваљујући којим активностима, колико су организацију коштале те активности, колико би организацију коштало да се штетни догађај заиста догодио, колико штете је спречено у односу на потенцијал опасности, и друго).

---

[225] Студија случаја је обухватила инцидент када је дошло до пада мреже у једној развијеној организацији. Одмах се посумњало на сервер, а истрага је показала да је на том уређају украдена *RAM* меморија. И ако је организација уложила знатна средства у технички део информационе безбедности, покушали су да уштеде на буџету намењеном физичкој безбедности. Из тих разлога су камере биле неисправне (то је било познато запослнеима у IT одељењу). *Towards a Conceptual Foundation of Physical Security, Case Study of an IT Department*, Journal of Safety and Security Engineering, Vol. 9, No. 2, 2019.

[226] Дијаграм односа улагања у механизме заштите и уштеде услед спречавања реализације напада, Марковић-Петровић, Д. Ј.: *Процена безбедносног ризика у индустријским системима даљинског управљања*, докторска дисертација, Саобраћајни факутлет, Универзитет у Београду, 2018. година, стр. 39., Доступно на: http://nardus.mpn.gov.rs/bitstream/handle/123456789/10602/Disertacija.pdf?sequence=1&isAllowed=y

Графикон број 9: ***Однос улагања у механизме заштите и уштеде услед спречавања реализације напада***



Организовањем самосталне пословне функције безбедности, проблем реалног буџетирања за ове потрене, на нивоу организације, у знатној мери се умањује и приближава се стварно потребном. Поставка да безбедност није трошак, него инвестиције организације (због смањења настанка штета) јесте теоријски исправан, али је у пракси проблематичан. Поред наведеног, те поставке су свесни обично власници или њихови представници капитала, дакле он је видљив на највишем нивоу управљања организације. Нижи нивои, а посебно средњи менаџмент, углавном су опредељени на успех пословне функције чијим радом руководе (који се у том конктексту може посматрати као алат за постизање личног успеха). Свест о заједничким циљевима припада организационој култури, и потребно је да организације улажу много напора да та свест буде на жељеном нивоу. Исто је и у области развоја безбедносне свести запослених, што нас још једном доводи до овог проблемског питања и феномена људског понашања у организацији.

3.3. Информациона безбедност у оквиру општих послова

Организовање послова заштите иформација у оквиру пословне функције која се бави општим, или административним пословима, један је од организационих облика који представља решење које има своје предности, али и своје недостатке.

Предност је свакако у томе што се послови безбедности налазе у оквиру једне пословне функције, о чему смо дискутовали у претходном моделу организованости, где је функција заштите ифнормација била распоређења у оквиру HR пословне функције, али су послови безбедности били груписани у једну целину.

Природа општих послова је таква да се односи на свакодневни живот организације, одакле овакво решење има предности у смислу боље интерне комуникације послова безбедности са другим пословнм фукцијама, у односу на неке друге моделе.

Безбедносне функције које се односе на заштиту запослених (енгл: *Personnel Security*), физичка безбедности и заштита информација нису у оквиру одговорности једног руководиоца, односно ове функције координира руководилац општих послова, чиме се добија додатни ниво у руковођењу пословима безбедности у организацији (што је био и случај са организовањем послова у HR-у), будући да свака од безбедносних функција има свог руководиоца, (а што није био случај када је руководилац безбедности сам координирао свим безбедносним функцијама).

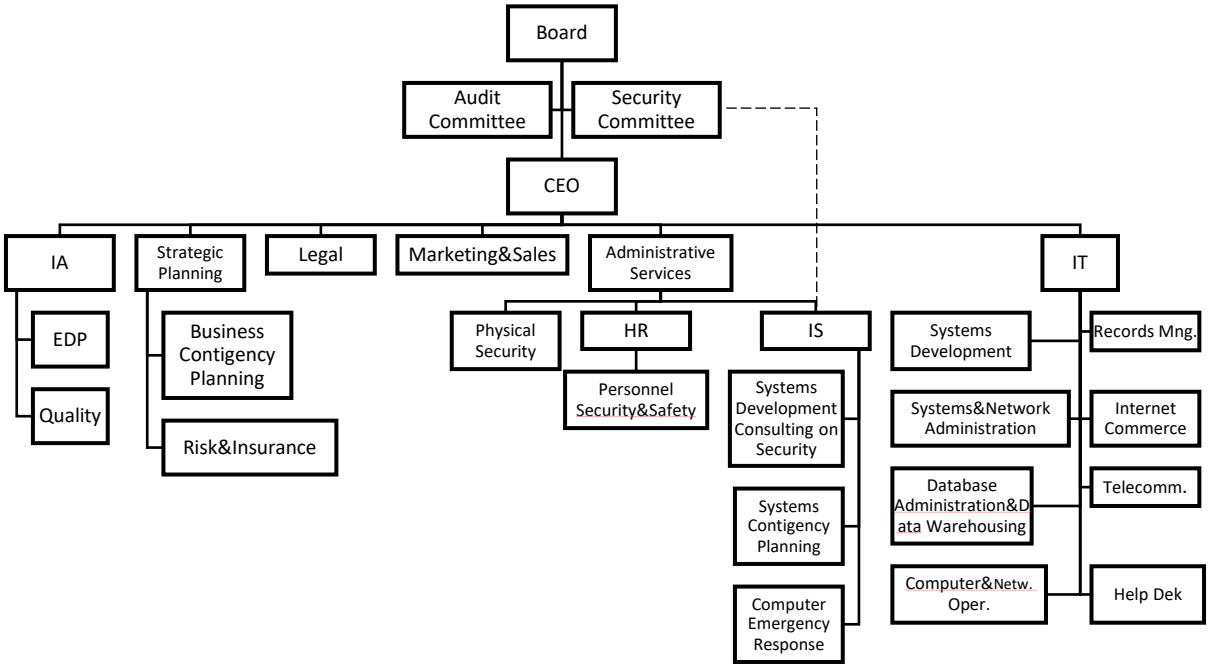
Слабост оваквог решења може бити избор менаџера који руководи општим пословима, у смислу да успешност његовор руковођења у знатној мери зависи од његових склоности и врсте образовања које има (да ли је техничке или нетехничке природе). Овакве ситуације се превазилазе тако што организације одређују додатне ресурсе да се руководиоцима општих послова приближе потребна знања која је потребно да има, како би разумео проблематику заштите информација, на једној страни, а на другој, да би разумео шта подразумева концепт безбедности. Исти проблем, са својим посебносима, сусрећемо увек када фукција безбедности нема директну линију рапортирања ка извршном нивоу организације.

Посебност административних послова, са аспекта безбедности, јесте управљање документацијом организације. Реч је о томе да савремено пословање, у складу са најновијом технолошком револуцијом, захтева од организација да архивирање своје документације обавља у складу са заком, што није новост, као и да обезбеди да се докуметнација чува у дигиталној форми.

Блискост са овом проблематиком, на оперативном нивоу, знатно олакшава ефикасност функције заштите информација, јер се у оквиру истог организационог дела (административних послова) обавља следеће:

- организовање архивских послова;
- физичко чување документације;
- уништавање документације;
- дигитализација документације;
- управљање дигиталном документацијом;
- чување архивске документације.

Схема број 11: ***Информациона безбедност у Одељењу општих послова***



Насупрот пороцесу дигитализације, организације и даље имају огроман број докумената који су на папиру. Претварање ових записа у дигиталну форму је процес који је у организацијама обилан и сталан. Коначно, поставља се и питање места где се толико обимна документација може физички сместити. Ово су, између осталог, разлози због којих се послови архивирања све чешће поверавају специјализованим организацијама које обављају ове послове као услужну делатност.

Послови заштите информација витално су заинтересовани за начин обављаља послова архивирања документације, одакле је ова чињеница може бити предност у избору оваквог модела организовања послова.

3.4. Информациона безбедност у оквиру послова стратегије и развоја

Специфичност овог модела организовања произилази из значаја стратегије и планирања као пословвне функције за извршни менаџмент, одакле се наглашава да организовањем заштите информација на овакав начин организација показује колико целокупно пословање зависе од компромитације инфорамација.

Витман и Маторд наводе да је овак модел пожељан углавном код организација које послују преко итнернета, као и код организација које се баве картичним пословањем (Схема број 12: *Информациона безбедност у Одељењу стратегије и планирања*).[227]

Недостатак видимо у раздвојености других функција безбедности од заштите информација, из разлога које смо навели у другим облицима организовања, када такође долази до оваквог распршивања безбедносне функције (одсуство холистичког приступа функцији безбедности), с тим да је се у овом моделу она разбија на чак три пословне области.

Не тако мала предност, према нашем мишљењу, у томе је што се у овом моделу физичка безбедност налази у оквиру послова одржавања, одакле се ставља нагласак на важност исправног функционисања безбедносне опреме и уопште – ставља се нагласак на важност техничке исправости свих система који омогућавају обављање основне делатности организације у строго дефинисаним амбијенталним условима (контрола приступа, против провала, CCTV, заштита од пожара, температура и влажност ваздуха, исправност техничких инсталација, превенција поплава и друго).

3.5. Информациона безбедност у оквиру правних послова

Овакав облик организовања, где су послови заштите информација смештени у правну пословну функцију, нису тако чести у пракси, али су одрживи и посебно се очекује да тек буду примењени у будућности, како наводе Витман и Маторд.[228]

Потенцијал овакве организације огледа се у блискости правних послова са нормативним уређењем послова безбедности, где смо из досадашег разматрања видели да је реч о једној од основних група мера које се примењују у заштити информација, поред мера физичко-техничке и логичке заштите (Схема број 13: *Информациона безбедност у Одељењу за правне послове*).

. Организације чије пословање зависи од информационе имовине, а не у првом реду од нформационог система, најпогодније су за примену оваквог модела организовања. Ауторска права, патенти, заштитни знакови и уопште интелектуална својина, ресурси су који се штите низом мера из области заштите информација, а са правне стране се по значају издвајају уговори о поверљивости.[229]

---

[227] Whitman, M., Mattord, H. J., *op.cit.*, стр. 176.
[228] *Ibid*

[229] Бројни су називи овог механизма заштите информација на енглеском језику, који су се одомаћили у пословној пракси код нас, па их из тих разлога наводимо, према следећем: *Non-Disclosure Agreement (NDA), Confidetiality Agreement (CA), Confidental Disclosure Agreement (CDA), Proprietary Informaton Agreement (PIA) i Secrecy Agreement (SA)*

Предност је и што се послови осигурања и управљања ризиком стављају у исту послвону функцију са заштитом информација, како смо већ претходно наведли у одговарајућем пословном моделу.

Схема број 12: ***Информациона безбедност у Одељењу стратегије и планирања***

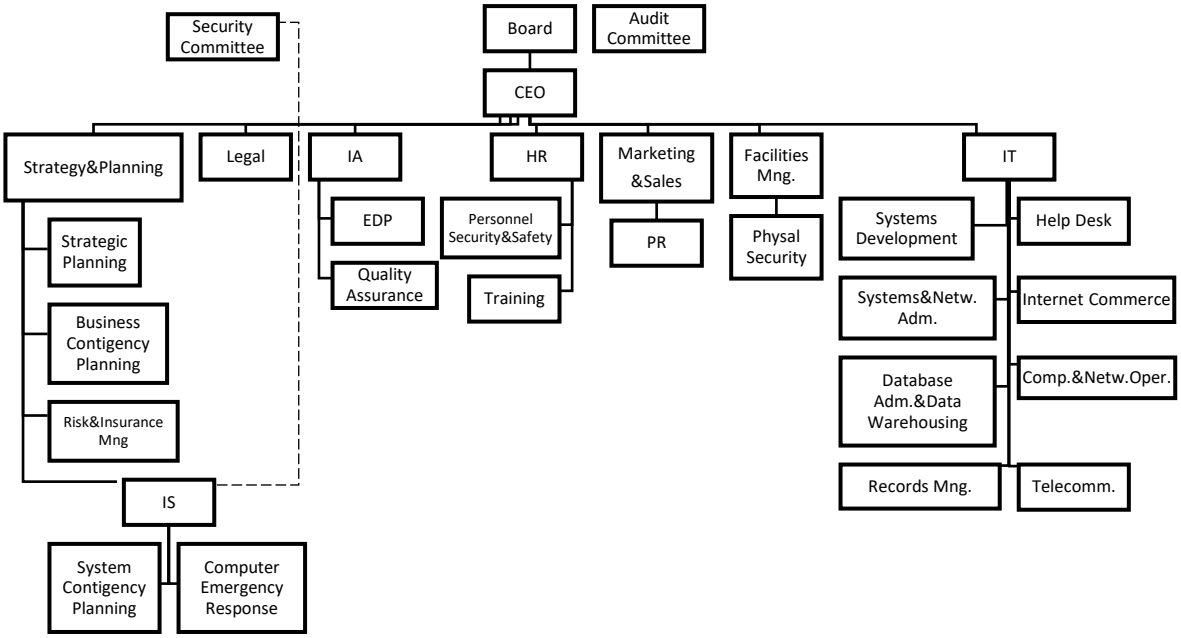
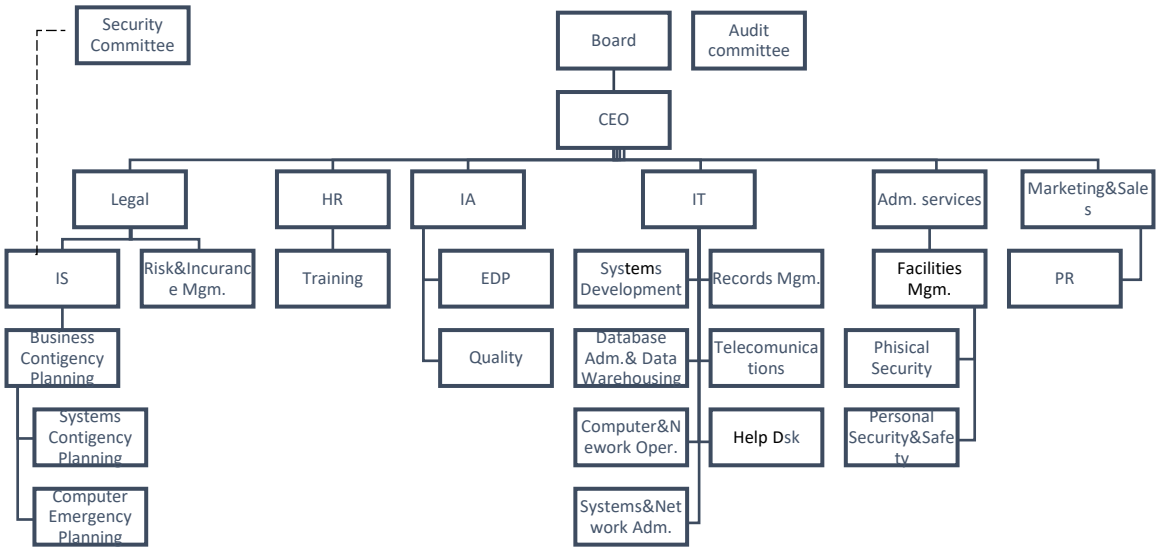


Схема број 13: ***Информациона безбедност у Одељењу за правне послове***



3.6. Информациона безбедност у пословима осигурања и управљања ризиком

Овај модел организовања послова безбедности носи са собом две врте предности и посебно је, због своје природе, примењив за банке и финансијске институције.

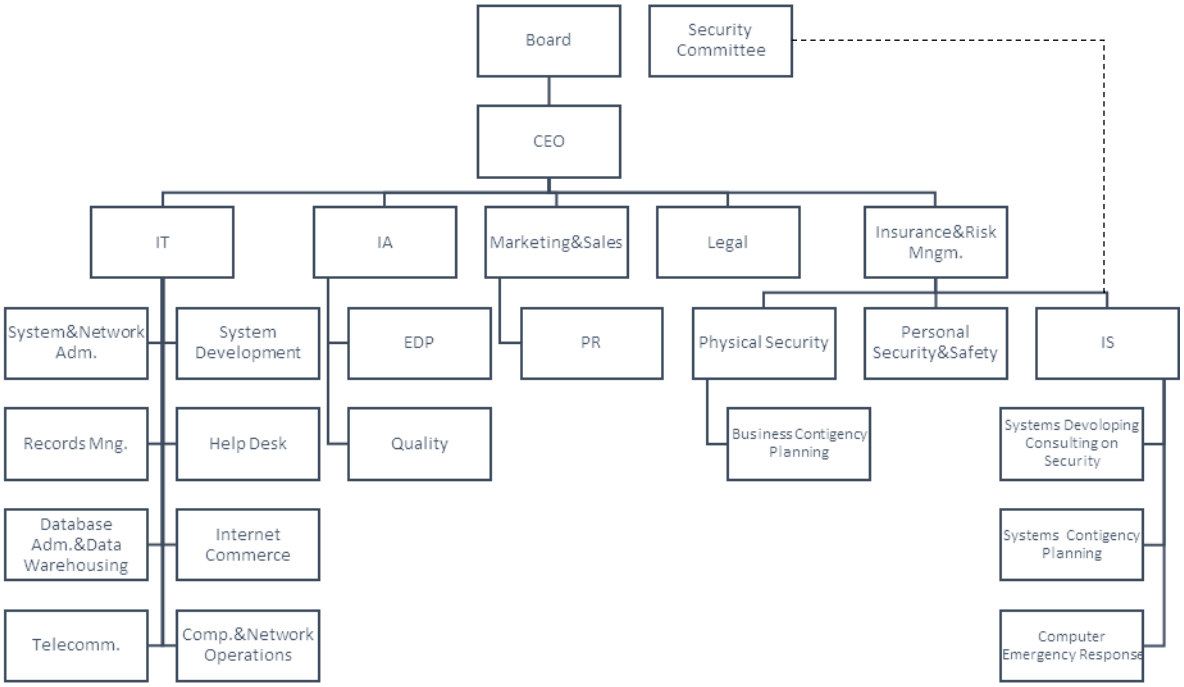
Прво, фукција безбедности је организована на једном месту у организацији, и у том смислу не долази до распршивања њених функционалности, која умањује ефикасност система заштите, како смо изнели у разматрањима претходних модела организовања.

Друго, сама природа послова послова управљања ризиком у организацији је блиска пословима безбедности, будући да је ризик појам који у овој пословној фукционалности има централно место. Функција безбедности у организацији бави се одговарајућим ризицима који се односе на организацију у којој је успостављена, док се фукција ризика односи на већу групу ризика којима је организација изложена, али обухвата и неке ризике којима се бави и сама безбедност. Такође, филозофија посматрања ризика као феномена, дели сличне погледе као и безбедност. У таквом приступу, потребно је из групе ризика издвојити оне који су од значаја за пословну фукционалност (пропознати их), систематизовати их, проценити њихов утицај на организацију, одредити кључне показатеље како би се ризици пратили, одредити мере заштите и радити њихову редовну евалуацију.

Још једна предност овакве организације налази се у чињеници да је пословна функција ризика усредсређена на посматрање целе организације и дељење информација са свим пословним функцијама, исто као и безбедност. Одатле ће у оваквим организационим моделима увек бити боља међусобна комуникација свих пословних функција и по питању безбедносних ризика. То је од посебног значаја за међусобне односе IT-а, Интерне ревизије, правне функције и послова безбедности, а посебно у кризним ситуацијама за организацију.

Пословна функција ризика у оганизацијама има предност у односу на друге, када је у питању безбедност, јер извршни менаџмент углавном има свест на високом нивоу од значају пословне функције управљања ризиком, одакле је комуникација са управљачким структурама олакшана и већу „специфичну тежину“.

Схема број 14: ***Информациона безбедност у овкиру пословне функције за осигурнање и управљање ризицима***



Посебно, од значаја за предмет нашег истеаживања, jeste чињеница да је ризик категорија који је неодвојив од пословања банака и финансијских институција, о чему ће у каснијим разматрањим бити више речи.

На овом месту желимо да наведемо, као додатњу аргументацију за претходн наведено о блискости ризика и безбедности, да је појам *оперативног ризика* дефинисан, као једна од петнаест категорија ризика које препознаје банкарско пословање и према којем банке имају обаезу према регулатору (НБС) да организују ове послове. *Оперативни ризик односи се на могућност настанка негативих ефеката на финансијски резултат и капитал банке који су последица пропуста (ненамерних и намерних) у раду запослених, неодговарајућих интерних процедура и прописа, неадекватног управљања информацијама и другим системима, као и услед непредвиђених екстерних догађаја. Оперативни ризик укључује и правни ризик.*[230]

Раније у тексту навели смо да ће према неким подацима у току 2020. године, на светском нивоу, бити потрошено око осам милијарди долара за потребе покривања полиса осигурања, које плаћају организације како би ублажиле евентуалне губитке насталих угрожавањем информација. Годину раније, тај износ је био пет милијарди долара. Бележимо да је реч о око 6.5% годишњих буџета који се троши за заштиту информција, као и да се тренд улагања у ову меру заштите брзо повећава, те да се очекује да ће тек доћи до раста

[230] Извор: Народна банка Србије, доступно на: https://www.nbs.rs/internet/cirilica/55/55_6/index.html

буџетирања компанија за потребе осигурања од штетних догађаја изазваних компромитацијом информација.

Ове чињение су још једна предносот организовања послова заштите информација у оквиру пословне функције осигурања и ризика, будући да интерна комуникација унутар исте пословне функције олакшава руководиоцима безбедности да се изборе за буџет и за ове потребе, онда када организација нема обевезе у овом смислу према регулатору.

3.7. Организовање заштите информација у другим пословним функцијама

Поред претходно наведених модела организовања послова заштите информација, који су наведени као најучесталији облици који се могу срести у пракси, предметни послови се могу организовати и на друге начине.

Избор одговарајућег модел зависи од више елемената, у које могу да спадају следећи: врста индустрије којој припада организација, национална култура (безбедносна култура), географски простор са својим економским особинама тржишта, нормативни оквир, величина организације, старост организације (да ли је пословни субјекат на почетку свог деловања или је присутан већ неко време на тржишту), степен криминалитета окружења, организациона култура, расположиви људски ресурси, пословни циљеви организације, величина буџета организације и други.

Безбедност не треба посматрати као готов производ, већ је то процес. Тај процес зависи такође од више елемената, услед чега се организовање послова заштите информација треба прилагођавати условима амбијента у којем се налази. Крајњи циљ организовања послова безбедности није само место у хијерархији организације, већ је то ефикасан заштитни систем. Постигнути ниво безбедности не значи да је организација достигла свој оптимум у организовању ових послова, јер се извори угрожавања и појавни облици претњи стално мењају и усложњавају, одакле и он треба да се прилагођава конкретним потребама и условима.

Полазећи од нашег предмета истраживања, заштите информација у банкама и финансијским институцијама, ми нећемо детаљније разматрати и друге могуће модела организовања ових послова, али ћемо навести да је у складу са претходно наведеним могуће да послови безбедности буду у оквиру следећих пословних функција, како наводе Витман и Маторд:[231]

- интерна ревизија;
- *Help Desk;*
- рачуноводство и финансије;

[231] Whitman, M., Mattord, H. J., *op.cit.*, стр. 179. – 182.

- *HR;*
- одржавање;
- *operations.*

4. Нормативно уређење заштите информација

Јовановић наводи да је право (правни поредак) комплексан феномен који садржи нормативни део, вредносни односно метаправни део и фактички односно социјални део. Нормативни део се састоји од правних норми и правних аката. *Правна норма је обавезно правило о понашању људи у друштву, загарантовано државним ауторитетом, односно институционализованом принудом*. Правна норма није исто што и члан или параграф једног закона или неког другог правног акта. Правна наука има за задатак да из различитих правних аката издвоји саставне делове једне правне норме. Примера ради, делови једне правне норме могу се налазити у различитим правним актима (законима, уредбама и сл,) – док се диспозиција, као правило о понашању налази у једном акту, дотле се санкција налази у неком сасвим другом акту.[232]

Ранђеловић разматра правну регулативу компјутерског криминала, посматрано кроз правну регулативу у међународној заједници и кроз правну регулативу високотехнолошког криминала у Републици Србији. У том смислу наводи активности које се обављају преко Организације уједињених нација, Организације за европску сарадњу и развој (ОЕЦД), Савета Европе и Европске уније, када је у питању међународни оквир. За сузбијање компјутерског криминала, када је у питању домаћа пракса, он наводи да је уређена међународним конвенцијама, законским и подзаконским актима, и наводи који су то правни акти.[233]

Путник наводи да се правна регулатива сајбер криминала одвија на више колосека (међународном и домаћем), а да је знатно више активности на међународном, него на националном и саморегулационом плану – што је и разумљиво, с обзиром на природу деликата у сајбер простору.[234]

Истраживањем иностране литературе и праксе, установили смо да се поред „правне норме“, под нормативним оквиром подразумева шири контекст, где се уважавају и међународни стандарди и примери добре праксе, као и препоруке, дакле све оно што представља амбијент једне организације у смислу организовања заштите информација.

[232] Јовановић, М.: *Правна норма*, предавање, Правни факултет, Универзитет у Београду, Доступно на: http://ius.bg.ac.rs/prof/Materijali/jovmio/Dokumenti/Pravna%20norma.htm
[233] Ранђеловић, Д.: *Високотехнолошки криминал*, Криминалистичко-полицијска академија, ЈП „Службени гласник“, Београд, 2013. година, стр. 309. – 336.
[234] Путник, Н.: *Сајбер простор и безбедносни изазови*, Факултет безбедности, Универзитет у Београду, 2009. година, стр.: 168. – 185.

Агенција Европске уније за сајбер/кибер безбедност (енгл: *The European Union Agency for Cybersecurity − ENISA*) под нормативним оквиром (енгл: *normative framework*) у заштити информација подразумева групу докумената и примера најбоље праксе који се односе на области:[235]

- питања заштите података/приватности;
- националне безбедности;
- грађанских и кривичних закона;
- корпоративног управљања и оперативне одговорности (питање Континуитета пословања);
- *Е* пословања;
- стандарда у области управљања ризиком и процене ризика (енгл: *Risk Management/Risk Assessment – RM/RA*).

Водич кроз информациону безбедност у Републици Србији[236], студија издата од стране Мисије ОЕБС-а у Србији, представља преглед стања сајбер безбедности код нас, са нагласком на стратешки и *нормативни оквир*. Полазећи од предмета истраживања нашег рада, овој студији даћемо више простора, будући да је рађена средином 2018. године, и да даје, по нашем мишљењу, добар преглед нормативног оквира области заштите информација.

Међународне обавезе се анализирају кроз принципе, стандарде и норме на које се Републике Србија обавезала (на основу стратешког избора чланства и сарадње са међународним и регионалним организацијама, иницијативама и механизмима, укључујући Европску унију (ЕУ), Организацију Северноатланског уговора, Организацију за европску безбедност и сарадњу и Уједињене нације.

Европска унија, има најразвијенији међународни оквир којим се уређује питање сајбер безбедности и приступа овом проблему са више аспеката: безбедносног, економског и политичког. До сада, највећи допринос је дала (већ споменута) Евроспка агенција за безбедност мрежа и и информација (*ENISA*), чија је једна од улога да ради заједно са државама чланицама ЕУ и приватним сектором на развоју ове области.

Први, кровни документ који је донела ЕУ је *Стратегија сајбер безбедности*[237], према којој државе чланице имају обавезу да утврде критичну инфраструктуру на својој територији и да Европској комисији доставе податке о ризицима, претњама и слабостима.

---

[235] Доступно на: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/normative-framework

[236] *Водич кроз информациону безбедност у Републици Србији* , Мисија ОЕБС-а у Србији, Unicom Telecom, IBM, Juniper, Грид студио, Београд, 2018. година, доступно на: https://www.osce.org/sr/mission-to-serbia/404258?download=true

[237] *Стратегија сајбер безбедности ЕУ*, 2013. година, доступно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

Истовремено је формирана, као пилот пројекат, *Информациона мрежа за упозоравање критичних инфраструктура* (енгл: *Critical Infrastructure Warning Information Network − CIWIN*)[238], чија је сврха размена информација о заједничким претњама, слабостима и одговарајућим мерама и стратегијама за смањење ризика, а приступ је омогућен и владама, организацијама и стручњацима из трећих земаља у оквиру формалне сарадње са ЕУ.

Безбедносна агенди ЕУ, набраја врсте сајбер криминала као једног од три кључна приоритета који захтевају хитно деловање, заједно са тероризмом и организованим криминалом, а где су банке и финансијске институције препознате као једна од најважнијих мета нападача.[239]

*Директива о мерама за високи заједнички ниво безбедносних мрежних и информационих система у ЕУ (*енгл: network and information systems – *NIS*) [240], познатија као *НИС директива*, где се позивају све државе чланице да пропишу основне стандарде безбедности и да формирају националне центре за превенцију безбедносних ризика у ИКТ системима (енгл: *computer emergency response team – CERT*), те да усвоје националне стратегије и планове сарадње у овој области. НИС директивом се такође одређује да безбедносне мере треба да буду засноване на принципу управљања на основу процене ризика, што треба да буде култура која се развија кроз регулаторне оквире, као и на основу пракси у различитим браншама. Овај документ представља основну контролну листу за сваку државу чланицу, а посебно земље кандидате, као што је наша земља. Такође, овај документ прописује да су државе чланице обавезне да одреде своју критичну инфраструктуру, према областима како се то у тексту наводи, где је такође сектор банкарства и финансијских услуга препознат као критичан.

Општа одредба Европске уније о заштити података о личности (енгл: *General Data Protection Regulation − GDPR*) бави се безбедносним, економским и политичким аспектима сајбер безбедности и одређује полазни оквир за усклађивање закона о приватности података. Примењује се без обзира на земљу о којој се ради или место у којем се налази привредно друштво, али се односи само на податке о личности и лицима који бораве у ЕУ. Допринос нормативном регулисању области заштите информација дале су и друге институције које се наводе у студији, а ми ћемо, полазећи од предмета нашег истраживања направити осврт на домаћи нормативни оквир.

Закон о информационој безбедности, представља кровни закон којим се регулишу мере заштите од безбедносних ризика у ИКТ системима, одговорности правних лица приликом управљања ИКТ системима и његовог коришћења, и одређује надлежне органе за спровођење мера заштите. Можда и најважније, полазећи од претходно наведеног о нормативи ЕУ, чини оснивање ЦЕРТ-а, тела задуженог за брзо реаговање у случају

[238] Доступно на: https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

[239] *The European Agenda on Security*, Strasbourg, 28.4.2015, доступно на: https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf

[240] *Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. Official Journal of the European Union L 194/1*., доступно на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

инцидента, као и за прикупљање и размену информација о ризицима за безбедност ИКТ система.

Уредба о утврђивању листе послова у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја, донета не на основу НИС директиве ЕУ.

Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја, уређује мере заштите ИКТ система у циљу прененције и минимизације штете од инцидента кји угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Уредба о ближем садржају акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедности, упућује на садржај акта о безбедности. РАТЕЛ је израдио огледни примерак овог документа и ми ћемо у касније разматрањима детаљније коментарисати овај документ.

Уредба о поступку достављања података, листи, врстама и значају инцидента и поступку обавештавања о инцидентима у ИКТ системима од посебног значаја, утврђује инциденте које је оператер дужан да пријави и одређује врсте инцидената.

Стратегија развоја информационе безбедности је донета за период од 2017. до 2020. године и подразумева доношење одговарајућег *Акционог плана*.

Канцеларија за информационе технологије и електронску управу, послове безбедности ИКТ система ставља на ниво Владе.

Закон о изменама Закона о информационој безбедности, уводи уместо Управе за заједничке послове републичких органа ЦЕРТ републичких органа

Упоредо са успостављањем нормативног оквира, развија се и неформални, оперативни оквир, који је успостављен радом *Петничке групе*. Она представља својеврсни мост између техничке заједнице и доносиоца одлука о политикама.

Мисија ОЕБС-а је подржала организацију прве сајбер бежбе, која је била усмерена на испитивање постојећих комуникацијских процедура, у случају сајбер инцидента.

5. Нормативно уређење заштите информација у организацијама

У досадашњем истраживању феномема заштите информација констатовали смо да иако она има стратешки значај за развој људске заједнице од њеног настанка, у савремено доба, задњом технолошком револуцијом која се догодила у глобалном сајбер простору, информације постају стратешки ресурс, а њихова природа нас приморава да са једне стране имамо потребу да их делимо са великим бројем корисника, а са друге стране осећамо потребу за њиховим рестриктивним приступом.

Са овом чињеницом суочавају се и све привредне организације, а посебно банке и друге финансијске институције.

Претходно смо видели норматививни амбијент заштите информација на државном нивоу, где је у циљу заштите информација модерно друштво организовало бројне међудржавне споразуме, законе, стандарде, активности и контроле. Неке од њих смо навели како би описали амбијент у којем су се нашле државе, па и Република Србија, како би организовале елементарне услове за функционисање привредног система, будући да без такве врсте комплементарности неби било могуће учествовати на међународном, па и домаћем, економскмо тржишту.

Слично као и државе, тако су се и привредни субјекти, а могуће и пре свега они, нашли у позицији да своја пословања, своје системе заштите, треба да прилагоде амбијенту у којем послују, а то данас сигурно нису локални нивои држава у којима послују, и ако привредни субјекти имају обавезу да се прилагоде и том амбијенту.

Ако на међудржавном и државном нивоу, постоје декларације, закони, инструкције, стандарди, који чине нормативни оквир у којем државе треба да се организују у погледу заштите информатичких ресурса, можемо рећи да и на, условно речено, нижем нивоу, такође постоји нормативни амбијент који је потребно разумети и према њему прилагоди своје активности.

У том смислу, а полазећи од предмета нашег истраживања, потребно је сагледати који су ту све елементи нормативног оквира који чини амбијент за пословање привредних субјеката, а пре свега, која је то методологија у организацији нормативног оквира присутна у њему, те каква је архитектура неопходних докумената потребна организацијама да би успоставиле ефикасан систем заштите информација.

Прегледом литературе, недвосмислено смо констатовали да се готово сви аутори слажу да се добри безбедносни програми заштите информација заснивају на Политикама (енгл: *policy*). Витман и Маторд наводе да иако су политике најјефтиније средство за контролу, њих је обично и најтеже применити, будући да зависе од мере у којој их прихвате запослени у организацији.[241]

Уједно, то би представљало још једно извориште нашег интересовања за предмет истраживања, будући да смо и сами наговестили у хипотетичком оквиру да свођење система заштите информација само на IT безбедност, или како други аутори, видели смо, често наводе на „технички“ аспект феномена заштите информација, резултира непотпуним безбедносним системом – у овом случају, резултира неприхватањем прокламованих мера (политиком) припадника организације у потпуности, одакле и наше интересовање за безбедносну културу као део организационе културе организације.

[241] Whitman, M., Mattord, H. J.: *Management of Information security*, Course Technology Cengage Learning, second edition, Boston, USA, 2008., стр. 108. – 113.

Основна правила за обликовање политика заштите информација су:

- никада не смеју да буду у супротности са законима;
- морају да буду у стању да буду одрживе на суду, уколико их неко оспорава;
- морају да буду ажуриране (да уважавају конкретне потребе и специфичности организације, наше је мишљење).

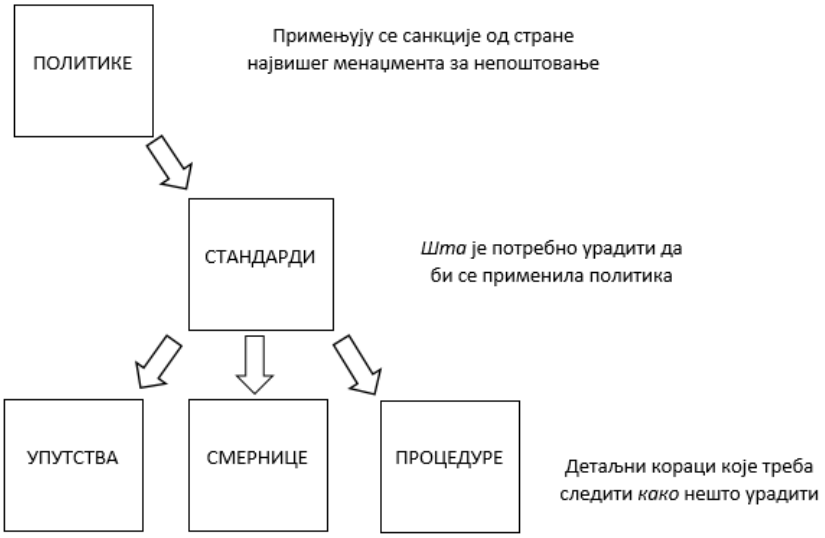
У пракси, сви се слажу да безбедносне политике није тешко дефинисати. Проблем је у њиховој примени, као што смо већ изнели. Аутори наводе да прихватању политика од стране организације помажу следеће смернице:

- морају се односити на организацију;
- менаџмент мора обезбедити адекватну поделу одговорности за поштовање заштите информација;
- крајњи корисници (дакле сви запослени) треба укључити у процес дефинисања политика;
- морају се писати јасним и концизним стилом, како њихова компликова стуктура неби деморалисала запослене да је примењују (ово се обично догађа када су политике засноване на компликованим техничким решењима или када су писане језиком који разуме само техничко особље).

Политике се дефинишу као план акције, слично као у политици, тако је и у пословном контексту. Она представља формалну изјаву управљачке филозофије организације у погледу заштите информација. Једном када се политике осмисле, дефинишу, одобре и примене, поступци који су потребни за реализацију прокламованог могу се надограђивати (спецификовати према проблему који документ обрађује) и даље применити. Политке су дакле скуп правила која одређују прихватљиво и неприхватљиво понашање у организацији. Конкретизација утврђене политике, даје се кроз друга документа, као што су: стандарди, процедуре, упутства, смернице и друго.

Стандарди су више детаљни од политика и одређују *шта је потребно тачно урадити* да би било у складу са политиком. У том смислу се могу одредити и техничке контроле које обезбеђују надгледање примене политике, као и написати припадајуће процедуре. *Упутства, процедуре и смернице* дају одговор на питање *како нешто урадити*, да би било сагласно политици.

Схема број 15: ***Однос политика, стандарда и других докумената***[242]



Политика заштите информација разликује се за сваку организацију појединачно, чак и када је у питању иста индрустрија, будући да је свако правно лице специфично у погледу многих елелемата, а посебно када је у питању њихова величина, интерна организација, технологија која се користи, организациона култура, безбедносна култура и друго.

Ипак, могу се пронаћи нека општа начела која ови документи треба да испуњавају, као што су:

- осврт на безбедносну филозофију у организацији;
- информације о структури информационе безбедности у организацији, као и подаци о појединцима који су у том смислу најодговорнији;
- потпуно дефинисану одговорност за безбедност свих учесника у организацији (сви запослени, пословни сарадници, консултанти, посетиоци и др.);
- потпуно дефинисану одговорност за безбедност за сваку улогу у организацији.

Да ова општа начела могу да варирају, у зависности од многих услова (национална култура, организациона култура, безбедносна култура организације, нормативни оквир амбијента, врста индустије и друго, како смо и навели у прегледу релевантних научних радова из предметне области, где смо видели да многи аутори истражују односе између ових и других променљивих, посебно у односу на безбедносну свест запослених), можемо примети у практичном остваривању послова заштите информација.

[242] Прирећено према Whitman, M., Mattord, H. J, *Op.cit.* стр. 112.

Реч је о томе да у индустрији безбедности не постоји општеприхваћена пракса о класификацији документације која се односи на заштиту информација, тако да се основни принципи, које смо претходно изнели, у начелу поштују, са повременим одступањима.

J. Кинари је истраживала проблем потребне документације за успостављање безбедносне политике у организацији.[243] Том приликом је прегледом литературе и анализом рада више аутора, дошла до закључка да не постоји јединствени став о устројству безбедносне документације, али да разлике у мишљењима нису суштинске, те да приступ овог проблема зависи од контекста (од конкретних услова организацијског амбијента).

Ауторка је проучила девет различитих приступа, у погледу хијерархијске уређености безбедносне документације, а према њиховој приоритизацији, којом приликом су документа која су представљала нормативни оквир била према следећем:

- Повеља (декларација) о безбедности (енгл: *Charter/Code of Conduct*)
- Политика безбедности (енгл: *Policy*)
- Безбедносни стандарди (енгл: *Standard*)
- Смернице из области безбедности (енгл: *Guideline*)
- Безбедносне процедуре (енгл: *Procedure*)
- Инструкције из области безбедности (енгл: *Instuction*)
- Контролне листе, алати и слично (енгл: *Tool, Control, Baseline etc*)

Различити извори су дали и различите ставове по питању приоритизације безбедносних докумената (Табела број 8: *Преглед приоритизације безбедносне нормативе за организације*).

Не улазећи у детаљнија разматрања овог истраживања, можемо да закључимо, да поред одређених различитости, постоје и сличности које су индикативне и могу да нам користе за будућа разматрања у нашем раду, а то је:

- безбедносне политике се неизоставни део нормативе у организацијама. Овај документ има највећи приоритет, у складу са претходно изнетим у нашем раду, уколико се занемаре декларативне (али не мање важне) „свечане изјаве“ о важности заштите информација
- стандарди су документи који по приоритету прате безбедносне политике, с тим да неки извори, који су у мањини, наводе да им претходе смернице, односно процедуре. Овај налаз нам може бити прихватљив са становишта контекста о којем смо претходно говорили (дакле приоритет у доношењу овог акта зависи од конкретне организације, нормативног амбијента, безбедносне културе организације и др.)

[243] Kinnari, J.: *Development of a Structured Security Document Framework*, Laurea University of Applied Sciences, Master's Thesis, Vantaa, Finland, 2013. Доступно на: https://www.theseus.fi/bitstream/handle/10024/57628/Kinnari_Johanna.pdf;jsessionid=7599D39C85C7600A43B55B320B786B8B?sequence=1

– смернице и процедуре се готово једнако често налазе на листи нормативног оквира, као и Стандарди, као документа са нижом приоритизацијом у нормативном оквиру заштите информација и са већим степеном конкретизације третиране области коју регулишу

Табела број 8: ***Преглед приоритизације безбедносне нормативе за организације***

	Charter/Code of Conduct	Policy	Standard	Guideline	Procedure	Instuction	Tool, Control, Baseline etc
Bacik		1	3	2	4	4	5
Baskerville& Siponen	1	2					
Brotby		1	2	4	3		5
Cannon		1	2	3	4		
Johnson	1	2	3	4	4		
Peltier	1	2	3	3	3		3
Peters	1	2	3	4	4		
SABSA	1	2	4		3	5	
Wahe	1	2	3	4	5		

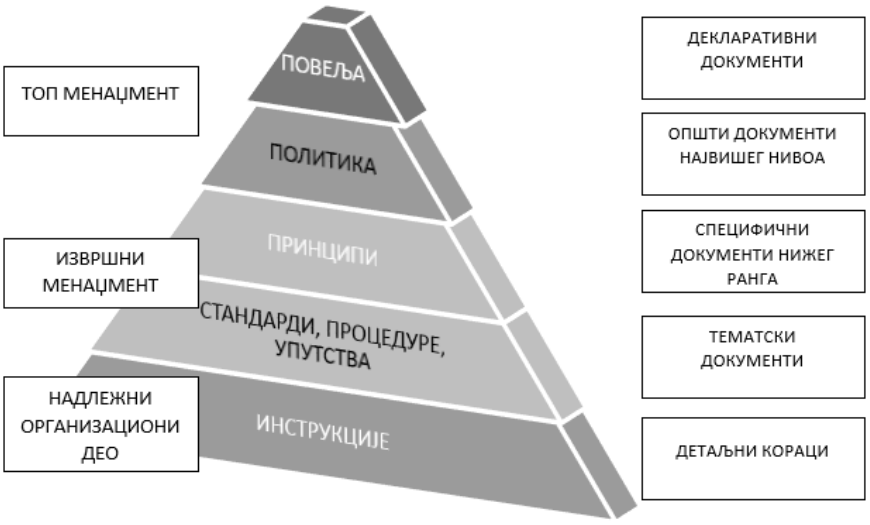
На основу изнетог, као и истраживања које је ауторка спровела (поред анализе литературе користила је интервју и анкету), архитектура нормативног оквира безбедносних докумената може се дати према следећем (Схема број 16: *Хијерархија нормативних докумената организације*).

За потребе нашег рада, и без амбиције да улазимо у детаљнију дискусију, јер сматрамо да није од кључног значаја за предмет истраживања, напомињемо да постоје извесна одступања када је у питању терминологија у називу докумената који чине нормативни оквир организација код остваривања заштите информација, како смо то до сада навели, и – домаће номенклатуре интерних аката који се доносе у организацијама. Тако се у домаћој пракси некада неће препознати значење термина као што су: политика, стандард (у смислу организацијског стандарда) и сл. Са друге стране, одлуке, правилници, наредбе, упутства, и други документи који могу бити садржани у нормативном оквиру, неће у потпуности бити препознати ако то искуство сведемо на раван искуства најбоље међународне праксе, када је

у питању заштита информација. Тако се може догодити да нека организација нема Политику заштите информација, али има Правилник који регулише ову област. Или – да организација нема Политику која регулише обавезу склањања документације на крају радног времена (енгл: *Clean Desk Policy − CDP*), али да има Правилник у којем су садржане овакве обавезе запослених, или Наредбу, односно други документ којим је суштински регулисан *Clean Desk Policy*.

Ми ћемо у даљем раду користи ону терминологију, како нам то наводе наши извори истраживања.

Схема број 16: ***Хијерархија нормативних докумената организације***[244]



6. Закључна разматрања поглавља

У овом поглављу разматрали смо значај који има заштита информација за пословање банака и финансијских институција, кроз објашњење основних појмова и сагледавање проблема истрживање кроз организациони и нормативни аспект остваривања ових послова.

Видели смо да значај области заштите информација извире из осетљивости коју оне имају за пословање и имовину ових правних субјеката. Штете које банке могу да претрпе, када су угрожене ове виталне вредности крећу се од оних подношљивих па до катастрофалних

[244] Прилагођено према: Kinnari J., *op.cit.*, стр. 38

штета због којих у питање може да дође и само даље пословање. Поред ових директних штета, информациони инциденти могу да доведу и до других, нематеријалних штета. Услед значаја које банке и друге финансијске институције имају за економију, о безбедности у том смислу воде рачуна и државе и државне заједнице, па се механизми за уређење ове области простиру и ван граница једне државе, што се види кроз регулисање нормативног оквира, као једне од мера која се примењују у заштити информација, о чему ћемо имати детаљнија разматрања у наредном поглављу.

На основу прикупљенихи података, видели смо да данас компаније, полазећи од природе феномена заштите иформација улажу не само у техничке мере заштите, већ и у оне које су нетехничке природе, а где се по свом значају и обиму њиховог улагања издваја следеће:

- тренинзи за повећање безбедносне свести запослених у заштити информација;
- усаглашеност организација са нормативом из области сајбер безбедности и заштите личних података о личности;
- *management of third party access;*[245]
- извођење вежби и симулација за сајбер нападе;
- улагање у полисе осигурања за случај сајбер напада;
- улагање у специјализовано особље за одбрану од сајбер напада.

У терминолошком смислу, данас постоје различити изрази за заштиту информација, од којих се поред наведеног, по учесталости у примени, издвајају информациона безбедност и сајбер безбедност, заједно са својим синонимом – *IT* безбедност.

Показали смо да се сајбер безбедност односи на безбедност било чега у сајбер простору, док безбедност информација подразумева заштиту информација − без обзира на подручје (дигитално или аналогно) где се налазе, одакле смо закључили да је безбедност (заштита, сигурност, итд.) информација надређени појам сајбер (кибер) безбедности.

Промишљајучи о феномену данас чешће употребе термина сајбер (*IT*) безбедности у односу на друге, покушали смо да допринесемо објашњењу ове појаве, предлажући следећи оквир за такву дискусију:

- у сајбер простору је доминантан енглески језик (лингва франка[246]), и то чак пет пута више од руског или кинеског језика и више него дупло у односу на шпански језик. У

[245] Дали смо израз на енглеском језику, будући да опсег појма није преводив на српски језик (израз као што би био превод „управљање приступа који има трећа страна“ није адекватан и могао би да наведе на погрешано тумачење појма), већ се може описати као област у којој је предмет посматрања однос који организације имају према својим добављачима, обично се мисли на спицијализоване услуге, као што су произвођачи софтвера, корисничких програма и слично, а имају потребу дневног приступању информационом систему организације.
[246] У онлајн верзији речника *Oxford Advanced Learner's Dictionary*, (лат: *lingua franca*) је дефинисан као језик који је усвојен као заједнички језик међу говорницима чији је матерњи језик различит. Користе га неизворни говорници, који имају различите лингвистичке и културне позадине. Не ради се о језику за посебне намене, нити о пицину или међујезику. Дакле, лингва франка је језик за комуникацију. Пиџин је језик сторен на бази речника и структуре једног језика. Користи се када нема заједничког језика између група.

ЕУ је други језик по броју људи који га говоре и представља један од службених језика за комуникацију администрације ЕУ (поред немачког и француског);

- стандарди, примери најбоље праксе и друга документа из области безбедности информација која се примењују у свету, како на енглеском говорном подручју, тако и у регионима где преовладавају други страни језици, изворно су на енглеском језику. Ова чињеница се посебно одражава у сфери самоучења стручњака, одакле се у говорном стручном језику примењују појмови који долазе одавде. На тај начин се ствара „нови језик“ струке, што искуствено опажамо код *IT* струке, а посебно у Републици Србији. Последично, и термини који се користе у сајбер безбедности, потичу из тог „новог језика“ струке;
- у области заштите информација, доминирају стандарди који долазе из техничког подручја, у односу на нетехничке стандарде;
- кадровска структура стручњака који се баве заштитом инфомација је таква да је њихово формално образовање углавном техничке природе (јер се безбедност информација везује за сајбер простор, оправдано или не), што је наша претпоставка коју тек треба доказати. Искуствено опажање нам говори у прилог овог тврдњи;
- нормативни оквир уређености заштите информација, када је у питању Република Србија и међународна сарадња, долази од стране институција и органа ЕУ, у највећем броју. Они стандарди и препоруке који потичу ван овог подручја, у складу са већ наведеним – на енглеском су језику, одакле се приликом превођења на српски језик све чешће користе термини створени у „новом језику“ струке;
- америчке софтверске компаније су убедљиво најбројније у свету, одакле се не може игнорисати интерес ширења тржишта и боље продаје производа (тиме и производа за заштиту информација) ове индустрије. Маркетиншки је прихватљивије област информација називати сајбер простором, јер и сами производи и услуге које нуди индустрија долазе претежно из сајбер простора;
- у САД термин сајбер безбедности (изнели смо већ да је чест синоним *IT* безбедност) је двоструко више у употреби од информационе безбедности, одакле се он последично, преко производа, трансфера знања, стандарда и друге документације која чини нормативни оквир заштите информација преноси даље, као неформални стандард струке.

У поглављу је направљен осврт на историјски развој области заштите информација, где смо разматрали, условно речено, модерно разумевање овог феномена који је наступио појавом рачунара, и у том смислу смо показали промене које су наступиле од шездесетих година двадесетог века до данас, када је у току нова технолошка револуција која ће опет, сасвим извесно, донети своје проблеме и нове мере заштите у остваривању заштите информација.

Вредност информације је довела до потребе да се савремено друштво определи за посебне напоре да организује мере заштите у овој области. Класификација тих мера се разликује у теоријском приступу, али ми смо за потребе нашег истраживања, сматрали да је прихватљиво да се све оне групишу у мере техничке и нетехничке природе. Такође, оне се могу груписати у зависности од своје природе на:

- нормативне мере (правне, организационе, кадровске);
- физичко-техничке мере;
- логичке мере; врло су ефикасне, али повлаче за собом трошкове који се не виде одмах, јер утичу на смањење расположивости и ефикасности рачунарских система, одакле се овим мерама мора да се приступа одговорно.

Са аспекта националне безбедности, мере у спровођењу заштите информација могу се посматрати на оперативном (тестирања информационих система), производном (тестирање хардвера и софтвера) и државном нивоу, где се захтева увођење *политике заштите информација* који би се односи на сва три наведена нивоа.

На основу искустава добре праксе, теорија се слаже да је приступајући проблему заштите информација пожељно применити вишеслојни модел заштите, који обухвата неколико аспеката (Цигурски[247]):

- физички (онемогућава физички приступ - физичко обезбеђење);
- технички (техничко обезбеђење - електронско обезбеђење; заштита од електромагнетног зрачења; идентификација, верификација и ауторизација приступа; системи за детекцију и спречавање напада; криптографија);
- организациони (организациона структура, дефинисање радног процеса, развој софтверских система, праћење смерница и стандардâ, планирање итд);
- кадровски (планирање и избор кадрова, руковођење, стручно усавршавање и безбедносно образовање итд.) и
- нормативни (закони, упутства, планови и друга регулатива која обавезује и прописује извршење неке радње и начин изршења те радње).

Том приликом, организацони, кадровски и нормативни аспект представљају *друштвени аспект заштите*, што се уклапа у претходно наведено о техничким и нетехничким мерама у заштити информација.

Без обзира на различите потребе организација, организационо и нормативно уређење заштита информација је увек присутно и зависи од више фактора, где смо ми полазећи од предмета нашег истраживања препознали као најважније:

- организациону (и безбедносну) културу;
- величину организације;
- износ буџета за потребе безбедности.

Такође, дали смо преглед основних функција које треба да буду укључене у програм заштите информација, којом приликом те функције нису обавезујуће да буду развијене у

[247] Цигурски, О.: *Информационе технологије у борби против тероризма*, Зборник Факултета цивилне одбране, Београд, 2005, стр. 179.

оквиру безбедносне функције организације, али је пожељно је имати их „негде“ у организационој структури, кроз остваривање неке од пословних функционалности система.

На основу свега изнетог, ми смо у овом поглављу размотрили неколико карактеристичних модела организовња послова у организацији, који се данас могу пронаћи у примени, којом приликом те моделе треба посматрати условно и више као начела и принципе него као конкретне и обавеујуће моделе. У том смислу анализирали смо следеће моделе организовања послова заштите информација:

- у оквиру IT послова;
- у оквиру пословне функције безбедности;
- у оквиру општих послова;
- у оквиру послова стратегије и развоја;
- у оквиру правних послова;
- у оквиру послова осигурања и управљања ризиком;
- у оквиру других пословних фукција.

Анализом наведених модела организованости послова заштите информација у организацији, ми смо дали коментар на особине понуђених модела, и том приликом смо дали одређене предности и уочене слабости. Такође, у вези нашег предмета истраживања, истакли смо потребу да послове безбедности треба организовати на такав начин да обухватају целу организациону структуру, али да не буду распршени по различитим пословним функцијама, а посебно да у области заштите информација не буду организовани тамо где је могућ и очекивајући сукоб интереса, као што је то био модел где су ови послови организовани у пословној функцији IT-а.

Наше је мишљење, и да избор одговарајућег модел зависи од више елемената, у које могу да спадају: врста индустрије којој припада организација, национална култура (безбедносна култура), географски простор са својим економским особинама тржишта, нормативни оквир, величина организације, старост организације (да ли је пословни субјекат на почетку свог деловања или је присутан већ неко време на тржишту), степен криминалитета окружења, организациона култура, расположиви људски ресурси, пословни циљеви организације, величина буџета организације и други.

Закључили смо да безбедност не треба посматрати као готов производ, већ да је то процес, који треба прилагођавати условима амбијента у којем се налази.

На крају, дали смо увод у поимање нормативног оквира заштите информација у банкама и финансијским институцијама, што ће бити посебно поглавље у нашем раду, где смо изнели да га треба посматрати на више колосека – међународном и домаћем. Такође, на нивоу организација, нагласили смо да нормативни оквир чине различити документи, са својим међусобним везама и односима, од који се издвајају безбедносне политике, стандарди, упутства, смернице, процедуре и друго, те смо у том смислу представили модел хијерархије нормативних докумената организације. Препознали смо да постоје извесна одступања када је у питању терминологија у називу докумената који чине нормативни оквир организација

код остваривања заштите информација, како смо то до сада навели, и – домаће номенклатуре интерних аката који се доносе у организацијама, али смо нагласили да у нашем раду немамо амбицију да решавамо овај проблем, већ да ћемо користити ону терминологију, како нам то наводе наши извори истраживања.

III НОРМАТИВНО УРЕЂЕЊЕ ЗАШТИТЕ ИНФОРМАЦИЈА У БАНКАМА И ФИНАНСИЈСКИМ ИНСТИТУЦИЈАМА

У оквиру поглавља о информационој безбедности навели смо да се мере заштите, према својој природи могу разврстати у мере нормативне заштите, физичко-техничке мере и логичке мере, где се под нормативним мерама подразумевају правни, организационе и кадровске активности. Нормативним мерама, утврђује се политика заштите, која одређује шта се сматра прихватљивим понашањем и какве су санкције за непримењивање прописаног.[248]

Такође, закључили смо да се нормативни оквиру заштите информација у банкама и финансијским институцијама треба посматрати у међународном, државном и локалном, контексту, односно на нивоу самих организација. Нагласили смо да нормативни оквир чине различити документи, са својим међусобним везама и односима, од који се издвајају безбедносне политике, стандарди, упутства, смернице, процедуре и друго, те смо у том смислу представили модел хијерархије нормативних докумената организације

Домаћа литература наводи да је правни оквир предуслов адекватне заштите информација, јер организацијама даје овлашћења и обавезе у погледу те заштите. Правни оквир чине прописи државних органа, на челу са Уставом и релевантним законима. Ти прописи чине нормативну основу, која даје обавезе и овлашћења правним лицима и чини темељ правне заштите заштите информација.[249]

1. Уставни и законски оквир заштите података

Устав Републике Србије, сврстава неповредивост тајности писма и друге комуникације и заштиту података о личности у основна људска и мањинска права. Прописује се да је тајност писама и других средстава комуницирања неповредива, а предвиђа и одступање од ових правила, на одређено време и на основу одлуке суда. Јамчи се заштита података о личности и одређује да се прикупљање, држање и обрада и коришћење података о личности одређује законом (Устав Републике Србије, 2006, чланови 41 и 42).

Уставне одредбе представљају основу за доношење закона којима се детаљније уређује начин остваривања људских права, а што је важно и за остваривање права која у овој области имају правна лица.

---

[248] Петровић, С.: *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004., стр. 20.

[249] Мандић, Ј. Г., Путник, Н., Милошевић, М.: *Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти*, Факултет безбедности, Универзитет у Београду, 2017. година, стр. 216.

Закон о безбедносно-информативној агенцији (БИА), предвиђа да директор Агенције може, ако је то потребно из разлога безбедности Републике Србије, својим решењем и на основу претходне одуке суда, да одреди према одређеним лицима (физичким и правним) предузимање одређених мера којима се одступа од изнетог начела неповредивости тајне писама и других средстава општења, што је проблематично са аспекта праксе и тумачења Европског суда за људска права, будући да нису дати ближи критеријуми који би утврдили круг физичких и правних лица према којима се мере могу одредити. На основу одлуке Уставног суда приступило се одговарајућим изменама и допунама, којима се ближе уређује да су посебне мере: тајни надзор за снимање и комуникације, надзор електронске или друге адресе, надзор и сниманње комуникације на јавним местима и местима којима је приступ ограничен или у просторијама, статистички електронски надзор комуникације и информационог система у циљу прибављања података о комуникацији или локацији коришћене мобилне терминалне опреме и рачунарско претраживање већ обрађених и других података и њихово упоређивање са подацима који су прикупљени. Чланом 14 Закона, прописује се да посебне мере могу одредити према лицу, групи или организацији за коју постоје основи сумње да предузима или припрема радње усмерене против безбедности Републике Србије, а околности указују да се на други начин те радње не би могле открити, спречити или доказати или би то изазвало несразмере тешкоће или велику опасност.[250]

Сличну судбину су доживеле одговарајуће одредбе Закона о БИА и *Закон о војно-обавештајној агенцији (ВОА)*, како наводе аутори, а према важећем решењу директор (или лице које он овласти) сада је овлашћено за предлагање, али не и за одлучивање примене мере, за шта је надлежан виши суд у седишту апелационог суда чијем подручју се припрема или је предузета радња чије је откривање, праћење или онемогућавање у надлежности ВБА.[251]

1.1. Законска регулатива прикупљања, обраде и заштите података

Закон о тајности података (2009), Закон о заштити података о личности (2009), Закон о заштити пословне тајне (2011), Закон о слободном приступу информацијама од јавног значаја (2004), представљају скуп релевантних закона којима се регулише обрада и заштита одређених врста података, чије нормативно уређење држава сматра неопходним и целисходним. Најважније врсте података у том смислу су:

- тајни подаци;
- подаци о личности;
- информације од јавног значаја;
- пословне тајне;
- професионалне тајне.

[250] Мандић, Г., Путник, Н., Милошевић, М., *op.cit.*, стр. 219. – 222.
[251] *Ibid.*

Поред наведеног, постоје и прописи који се баве другим материјама, али појединим одредбама пружају правну заштиту извесним категоријама података (*Кривични законик, Службени гласник РС, 2005; Законик о кривичном поступку, Службени гласник РС, 2011; Закон о информационој безбедности, Службени гласник РС, 2016; Закон о привредним друштвима, Службени гласник РС, 2011; Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, 2005*).[252]

1.2. Тајност података

Закон о тајности података прописује одређивање и заштиту тајних података који су од интереса за Републику Србију (области су: национална и јавна безбедност, одбрана, унутрашњи и спољни послови), а прате га подзаконски прописи којима се ближе уређује начин остваривања наведеног (*Уредба о начину и поступку означавања тајности података, односно докумената, Сл. гласник РС, бр. 8/11, Уредба о посебним мерама физичко-техничке заштите тајних података Сл. гласник РС, бр. 97/11 и др.*).

Полазећи од предмета нашег истраживања, значајно је да напоменемо да Закон о тајности података одређује значење појединих појмова и терминологије у овој области. Тако се одређује појам податка од интереса за Републику Србију, а тајни податак се дефинише као његова посебна врста. Податак од интереса за Републику Србију јесте *сваки податак или документ којим располаже орган јавне власти, који се односи на територијални интегритет и сувереност, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње послове и спољне послове*, али сви они нису истовремено и тајни подаци. Они се одређују законом, другим прописом или одлуком надлежног органа, мора бити донесен у складу са законом, одређен и означен одређеним степеном тајности.

Да би податак постао тајни, потребно је да постоји правни основ и да се спроведе поступак одређивања тајности података. Овим поступком утврђује се степен тајности и рок о истом.

Тајни податак може да прогласи *орган јавне власти* (државни орган, орган територијалне аутономије, орган јединица локалне самоуправе, организација којој је поверено јавно овлашћење, као и правно лице које оснива државни орган или се финансира у целини, односно претежним делом из буџета, а који поступа са тајним подацима, односно који их ствара, прибавља, чува, користи, размењује или на други начин обрађује).[253]

Такође, орган јавне власти су дужни да чувају и стране тајне податке, а то су они који су поверени Републици Србији, од стране других држава или међународних организација, уз обавезу да их чувају као тајне. Ово се односи и на тајни податак који настане у сарадњи

[252] *Ibid.*, стр. 223.
[253] *Ibid.*, стр. 224. – 225.

наше државе са другим међународним субјектима, а у складу са претходним међународним споразумом.

Службена лица која могу да прогласе тајност података под условима Закона о тајности података су: председник Народне скупштине, председник Републике, председник Владе, руководилац органа јавне власти, изабрани, функционер органа јавне власти (под одређеним условима) и лице запослено у органу јавне власти које је писмено овлашћено од стране руководиоца тог органа.[254]

Податак може да има један од следећих степена тајности:

- државна тајна (неотклоњива тешка штета по интересе Републике Србије);
- строго поверљиво (тешка штета по интересе Републике Србије);
- поверљиво (штета по интересе Републке Србије);
- интерно (спречавање могућности настанка штете за рад, обављање задатака и послова органа јавне власти који их је донео).

У циљу избегавања апстрактности дефиниције појединиих степена тајности донесени су:

- *Уредба о ближим критеријумима за одређивање степена тајности државна тајна и строго поверљиво* (Службени гласни РС, 2013);
- *Уредба о ближим критеријумима за одређивање степена тајности поверљиво и интерно у БИА-и*, (Службени гласник РС, 2013);
- *Уредба о ближим критеријумима за одређивање степена тајности поверљиво и интерно у МУП-у*, (Службени гласни РС, 2013);
- *Уредба о ближим критеријумима за одређивање степена тајности поверљиво и интерно у Канцеларији Савета за националну безбедност и заштиту тајних података* (Службени гласник РС, 2013);
- *Уредба о ближим критеријумима за одређивање степена тајности поверљиво и интерно у Министарству одбране*, (Службени гласник, 2013);
- *Уредба о ближим критеријумима за одређивање степена тајности поверљиво и интерно у органима јавне власти*, (Службени гласник РС, 2013).

Физичко или правно лице, да би добило право приступа тајном податку, потребно је да се испуне законски услови, а закон регулише који су услови, као и који су изузеци могући (издавање сертификата, претходна безбедносна провера и друго). Сертификат издаје Канцеларија Савета за националну безбедност и заштиту тајних података.[255]

Прописане су и опште мере заштите, и оне обухватају следеће:

- одређивање степена тајности;
- процену претње за безбедност тајног податка;
- одређивање начина коришћења и поступања са тајним податком;

[254] *Ibid*
[255] *Ibid,* стр. 229. – 233.

- одређивање одговорног лица за чување, коришћење, размену и друге радње обраде тајног податка;
- одређивање руководиоца тајним подацима, укључујући и његову безбедносну проверу у зависности од степена тајности податка;
- одређивање посебних зона, зграда и просторија намењених заштити тајних података;
- мере физичко-техничке заштите тајног податка, укључујући и постављање техничких средстава заштите, утврђивање безбедносне зоне и заштиту ван ње;
- мере заштите ИКТ (информационо комуникационих технологија) система;
- мере криптозаштите;
- заштитни режим радних и формацијских места, у оквиру акта о унутрашњем уређењу и систематизацији радних места;
- утврђивање посебних програма образовања и обуке за потребе обављања послова заштите тајних података;
- друге опште мере одређене законом.

Наведене мере могу да се класификују на физичко-техничке, административне/нормативне/организационе, персоналне и информационе. *Уредба о посебним мерама физичко-техничке заштите тајних података* (Службени гласник РС, број 97/11) одређује да се тајни податак чува, користи и обрађује у просторији, односно простору који је одређен као безбедна зона и има одговарајућу безбеднону опрему, односно одговарајућа средства техничке заштите.[256]

Безбедност тајних података у ИКТ системима је регулисана *Уредбом о посебним мерама заштите тајних података у информационо-телекомуникационим системима*, Службени гласник РС, број 53/11.

Уредба предвиђа следеће мере заштите:

Техничке мере, односе се на: физичку заштиту објеката (простора), против пожарну заштиту, обезбеђивање и заштиту опреме, заштиту програмске подршке, заштиту мреже.

Организаџоне мере се односе на: организацију технолоигје рада у систему при пројектовању, утврђивање поступака у случају ванредних околности и остале услове.

Уредба препознаје и безбедносне режиме у којима ИКТ систем ради у сврху заштите тајних података, кроз различите нивое, и то: селективан, неселективан и са више нивоа. За прва два нивоа је потребан сертификат за приступ тајним подацима највишег степена тајности (у зависности да ли се приступа свим или само делу података).

Члан 10 Уредбе регулише да ради одржавања безбедности система морају да се спроводе различите мере, као и примењивање нових техничких и програмских средстава у систему у

[256] *Ibid*, стр. 234.

складу са одговарајућим техничким стандардима СРПС ИСО/ИЕЦ 27001 и СРПС ИСО/ИЕЦ 17799.[257]

Члан 11 Уредбе прописује да се преносива информационо-телекомуникациона средства која се користе у систему сматрају тајним податком и да се могу укључити у систем само ако је претходно извршена провера могућег угрожавања система од стране стручних лица – што је посебно значајно са становишта безбедносне културе.

Унутрашња контрола, која може бити и ненајављена, потпуна или делимична, регулисана је *Уредбом о посебним мерама надзора над поступањем са тајним подацима* (Службени гласник РС, бр. 90/11), чиме се регулише непосредан увид и провере у вези са спровођењем мера заштите тајних података.

Закон о тајности података, Члан 35 регулише чување, преношење и достављање тајних података, док Члан 36 говори о обавези обавештавања у случају да је дошло до губитка, крађе, оштећења, уништења или неовлашћеног откривања тајних података.

Достављање тајних података на основу уговорног односа (тзв. *индустријска безбедност*), где је реч о уступању тајних података субјекту који нема статус органа јавне власти, регулисано је тако да овлашћено лице може да достави тајне податке другим правним или физичким лицима, по основу уговорног односа, уколико испуњава одређене услове, и то (Члан 46, Закон о тајности података):

- ако су испуњени организациони и технички услови за чување тајних података;
- ако је извршена безбедносна провера (лица која приступају тајним подацима) и издати сертификати;
- ако се писаном изјавом лица изјасне да су упозната са овим законом и другим прописима који уређују чување тајних података и обавежу се да ће са тајним подацима поступати у складу са прописима.

Ако им је приступ неопходан ради реализације послова предвиђених уговором

Индустријска безбедност је ближе одређена *Уредбом о посебним мерама заштите тајних података који се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа* (Службени гласник РС, 63/13).[258]

Организациони услови су у смислу овог акта су организација процеса рада, заштита приступа тајним подацима, заштита од неовлашћеног коришћења тајних података, одређивање одговорног лица задуженог за спровођење мера заштите, као и утврђивање поступка у случају ванредних и хитних околности.

Технички услови, односе се на физичко-техничку заштиту простора, против пожарну заштиту, заштиту тајних података прилиом преношења и достављања изван просторија у

[257] *Ibid*, стр. 237.
[258] *Ibid*, стр. 239.

којој се чувају, транспорт тајних података, обезбеђивање и заштиту ИКТ средстава којима се врши преношење и достављање тајних података и спровођење мера криптозаштите.[259]

Уредбом је дефинисан поступак закључења и реализације поверљивог уговорног односа, као и припремне активности и начин спровођења преговора (Члан 7), где је овлашћено лице дужно да спроводе, у случају да су тајни подаци означени са државна тајна, строго поверљиво и поверљиво, читав низ радњи (Члан 9), као што је:

- да ли је неопходан приступ тајним подацима ради реализације посла;
- да ли правно лице има одговарајући сертификат;
- да ли физичка лица имају потребне сертификате;
- да ли је простор у којем ће се чувати подаци опремљен у складу са прописом који уређује посебне мере физичко-техничке заштите тајних података;
- начин чувања, евидентирања и архивирања тајних података;
- начин вршења умножавања тајних податка;
- поступак уништавања тајних података;
- да ли постоји евиденција улаза излаза лица и возила, и друго.

Чланом 10 Уредбе уређују се обавезе правног или физичког лица које закључује поверљив уговор. Члан 11 предвиђа обавезе у случају раскида уговора (враћање докумената и материјала са тајним подацима и слично).[260]

Полазећи од предмета нашег истраживања, сматрамо да Уредба о посебним мерама заштите тајних података који се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа, може да послужи као образац за израду корпоративних аката, невезано што се ниво њихових осетљивих информација не односи експлицитно на изнета законска решења и одредбе подзаконских аката које смо навели, о чему смо раније у тексту већ напомињали кроз навођење значаја примене добре праксе, у остваривању заштите информација.

1.3. Заштита пословне тајне

Закон о заштити пословне тајне (Сл. Гласник РС, бр. 72/11) регулише правну заштиту пословне тајне од радњи нелојалне конкуренције.[261]

Пословна тајна штити податке од значаја за пословање организација, како што су: форумуле, методи, цртежи, пројекти, а полазећи од нашег предмета истраживања и посебно финансијски, економски и други подаци, информације о новим производима и слично.

[259] *Ibid*
[260] *Ibid,* стр. 241. – 243.
[261] *Ibid,* стр. 244. – 249.

Чланом 2 Закона, заштита пословне тајне гарантује се домаћем или страном правном или физичком лицу, а за лице које контролише коришћење пословне тајне законодавац користи термин *држалац пословне тајне*.

Пословна тајна је било која информација која има комерцијалну вредност зато што није опште позната, нити је доступна трећим лицима која би њеним коришћењем или саопштавањем могла остварити економску корист, и која је од стране њеног држаоца заштићена одговарајућим мерама у складу са законом, пословном политиком, уговорним обавезама или одговарајућим стандардима у циљу очувања њене тајности, а чије би саоштевање трећем лицу могло нанети штету држаоцу послове тајне.[262]

Мере заштите пословне тајне могу бити:

- физичко-техничке;
- административне;
- персоналне;
- информационе.

Законодавац предвиђа да неке нформације не могу бити пословне тајне (прикривање кривичног дела, прекорачење овлашћења, злоупотреба службеног положаја или други незаконит акт), као и оне које су посебним законима прописане да не могу представљати пословну тајну.

Уколико неки носач података садржи тајне податке и пословну тајну, он се штити као тајни податак, што може бити случај код јавних предузећа и привредних друштава које оснива или финансира држава − и штити се одредбама закона који уређује тајност података.

Значајно је да овај Закон не регулише шта је то индустријска шпијунажа, али говори о радњама супротним добрим пословним обичајима, под којима се подразумева свака радња предузета у циљу утакмице на тржишту којом се наноси или се може нанети штета конкуренту. Радње супротне добрим пословним обичајима сматрају се незаконитим када су предузете у оквиру индустријских или комерцијалних активности, а имају за последицу отривање, прибављање, односно корипћење информације која представља пословну тајну, без сагласности држаоца пословне тајне и на начин супротан закону. Ово законодавац назива нелојалном конкуренцијом и спецификује их према следећем (Члан 8 став 2):

- повреда уговорних одредаба и чување пословоне тајне;
- злоупотреба пословног поверења;
- индустријска или комерцијална шпијунажа;
- превара;
- навођење на неку од претходно наведених радњи;

[262] *Ibid*

- прибављање информације која представља пословну тајну од стране трећих лица која знају или су била дужна да знају да та информација представља пословну тајну и да је прибављана од лица у чијем је законитом поседу.

Законом се прописује грађанскоправна и привредноправна заштита лицима која су оштећена делима нелојалне конкуренције. Грађанскоправна заштита је регулисана на таква начин да њен држалац може тужбом да покрене поступак пред судом и да захтева следеће:

- престанак радњи које воде ка компромитацији пословне тајне и забрану незаконитог прибављања, коришћења или откривања пословне тајне;
- спречавање промета, одузимање или повлачење из промета, измену или уништавање свих предмета који садрже информације које представљају пословну тајну;
- искључење тог лица као члана привреднор друштва, ако је то случај;
- раскид радног односа, ако је то лице запослено у правном лицу;
- објављивање пресуде у јавном гласилу о трошку туженог.

Члан 13 предвиђа и изрицање привремене мере (одузимање или искључење из промета предмета који садржи пословну тајну или који су настали повредном пословне тајне, средства за производљу тих предмета, односно меру забране насвљања започетих радњи којима се врши или би се могла извршити повреда пословне тајне.

Аутори наводе да је необично да одавање пословне тајне предстсавља кривично дело, а индустријска шпијунажа привредни преступ, која је лакша категорија кажњивог деликта. Они наводе да амерички федерални закон о индустријској шпијунажи (из 1996. године) јасно инкриминише злоупотребе пословне тајне уколико је умишљај починиоца уперен ка стицању користи за иностраног субјекта. Наш Закон не дефинише шта се сматра индустријском шпијунажом, док КЗ не познаје овај појам, те не постоји законски ослонац за кажњавање дела повреде пословних тајни са елементом иностраности. [263]

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

Заштита података о личности обезбеђује се сваком физичком лицу, без обзира на држављанство, расу, вероисповест, језик, националну припадност и друго.

Послове заштите података о личности обавља *Повереник за информације од јавног значаја и заштиту података о личности*, као самосталан државни орган, независан у вршењу своје дужности.

Закон о заштити података о личности (Сл. гласник РС, 97/08, 104/09, 68/12 и 107/12) регулише област обраде података о личности, заштиту права лица чији се подаци

[263] *Ibid*

прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним судом за заштитиу података о личности, као и друга питања.[264]

Податак о личности је свака информација која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације. Физичко лице је човек на кога се односи податак, чији је идентитет одређен или одредив на основу личног имена, ЈМБГ броја, адресног кода или другог обележја његовог физичког, психолошког, духовног, економског, културног или друштвеног идентитета.

Члан 3 Закона одређује обраду података као сваку радњу предузету у вези са подацима, у шта се убрајају: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, отривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин.

Руковалац података је физичко или правно лица, односно орган власти који обрађује податке.

Обрађивач података је физичко или правно лице, односно орган власти, коме руковалац на односу закона или уговора поверава одређене послове у вези са обрадом.

Корисник података је физичко или правно лице, односно орган власти, који законом или по пристанку лица овлашћеног да користи поадтке.

Збирка података је скуп података који се аутоматизовано или неаутоматизиовано воде и доступни су по личном, предметном или другом основу, независно од начина на који су похрањени и места где се чувају.

Централни регистар збирке података јесте евиденција коју чини регистар збирки података и католог збирки података коју води Повереник. Централи регистар је јаван и обавезно се објављује путем интернета. Повереник једном годишње објављује попис збирки података у Службеном гласнику Републике Србије.

Закон препознаје *нарочито осетљиве податке о личности* (како што је национална припадност, раса, пол, језик, вероисповест и друго). Обрада ових података мора бити посебно означена и заштићена мерама заштите. Према Члану 16, Повереник има право увида у податке и провере законитости обраде по службеној дужности или по захтеву лица,

[264] *Ibid,* стр. 249. – 265.

односно руковаоца. Начин архивирања и мере заштите нарочито осетљивих података још увек није регулиса подзаконским актом, што представља пропуст.[265]

Члан 19 Закона одређује шта све лице има право да зна, као што је: да ли руковалац обрађује податке о њему, које податке обрађује, од кога се прикупљају подаци (извор података), у које сврхе, по ком правном основу, у којим збиркама се налазе подаци о њему, ко су корисници, које податке користе, коме се подаци преносе и друго.

Закон регулише обавезу вођења евиденција о збиркама података, које имају сви руководиоци, где је дужан да пре започињања обраде, односно успостављања збирке података, достави Поверенику обавештење о намери успостављања збирке података.

Уредба о обрасцу за вођење евиденције и начину вођења евиденције о обради података о личности (2009.), прецизира обавезе вођења евиденција у погледу образаца за вођење евиденција и начине њиховог вођења. Према овом акту, евиденција података о личности може се водити ручно или средствима за аутоматску обраду података, ако посебним законом није другачије одређено.

Законом о слободном приступу информацијама од јавног значаја (Сл. гласник РС, бр. 120/04, 54/07, 104/09 и 36/10), уређују се права приступа информацијама од јавног значаја којима располажу органи јавне власти, ради остварења и заштите интереса јавности да зна и остварења слободног демократског поретка и отвореног друштва. Члан 5 Закона утврђује право сваког лица да му буде саопштено да ли орган власти има одређену информацију од јавног значаја, односно да ли му је она доступна, као и да му се информација од јавног значаја учини доступном тако што ће му се омогућити увид у документ који садржи информацију од јавног значаја, право на копију тог документа, као и право да му се, на захтев, копија документа упути поштом, факсом, електронском поштом или на други начин (осим ако тражилац злоупотребљава права на приступ информацијама од јавног значаја, ако је тражење неразумно, често, када се понавља захтев за истим или већ добијеним информацијама или када се тражи превелики број информација).

[265] Корисничко име и лозинка за приступ информационом систему *Covid*-19 били су осам дана јавно доступни на сајту једне здравствене установе, одакле је овим подацима могао да приступи било ко. Информациони систем *Covid*-19 основала је Влада Републике Србије како би вршила епидемиолошки надзор за време епидемије. У бази су били подаци о излеченим, преминулим, тестираним и особама којима је изречена мера самоизолације. Систем, између осталог, садржи личне и здравствене податке, детаље клиничких испитивања, информације о лечењу и др. Требало би да су доступни надлежнима у Министарству здравља, Канцеларији за информационе технологије Владе, Министарству унутрашњих послова, Војсци и Институту за трансфузију крви. Доступно на: https://www.danas.rs/bbc-news-serbian/korona-virus-i-onlajn-bezbednost-kako-su-korisnicko-ime-i-lozinka-za-informacioni-sistem-covid-19-zavrsili-na-internetu/

Орган јавне власти може тражиоцу да онемогући остваривање права на приступ информацијама од јавног значаја под одређеним околностима, поред наведеног, у смислу разликовања тајног податка и информације од јавног значаја.

1.5. Нормативни оквир информационе безбедности

У области заштите података велики значај имају прописи којима се регулишу основи информацијског система Републике Србије и друга питања у вези примене информационо-комуникационих технологија у свакодневном животу, а то су:

- *Закон о информационом систему Репубике Србије* (Службени гласник РС, бр. 12/96);
- *Закон о ауторским и сродним правима* (службени гласник РС, бр. 104/09, 99/11, 119/12 и 29/16);
- *Закон о електронским комуникацијама* (Службени лист РС, бр. 44/10, 60/13 и 62/14);
- *Закон о електронском потпису* (службени гласник РС, бр. 135/04);
- *Закон о забрани дискриминације* (Службени гласник РС, бр. 22/09);
- *Закон о заштити потрошача* (Службени гласник РС, бр. 73/10 и 6/16).

Овим прописима дефинишу се основи заштите података употребном ИКТ, а стварају се основе система превенције високотехнолошког криминала.

Закон о ифнормационој безбедности (2016. године) одређује да се овим актом уређују мере заштите од безбедносних ризика у ИКТ системима, одговорности правних лица приликом управљања и коришћења ИКТ система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.[266]

Информационо-комуникациони систем, према овом акту, је дефинисан као технолошко-организациона целина која обухвата:

- електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
- уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарских програма;
- податке који се похрањују, обрађују, претражују или преносе помоћу средстава дефинисаних законом, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКТ системом.

[266] *Ibid,* стр. 265. – 274.

Носилац права и обавеза у овој сфери је означен као *оператер ИКТ система*, као правно лице, орган јавне власти или организациона јединица органа јавне власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности.

Информациона безбедност је скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.

Расположивост података одређује се као својство које значи да је податак доступан и употребљив на захев овлашћеног лица онда када им је потребан.

Аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да ту радњу извршио.

Интегритет значи очуваност изворног садржаја и комплетности података.

Тајност је својство које значи да податак није доступан неовлашћеним лицима.

Непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи.

Ризик се односи на могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавање исправности функционисања ИКТ система.

Управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризиsи остану у прописаним и прихватљивим оквирима.

Инцидент је унутрашња или спољна околност или догађај коим се угрожава или нарушава информациона безбедност.

Закон дефинише и друге термине које користи, а ми их нећемо појединачно разматрати, јер смо приказали оне који се односе на наш премдет истраживања. У том смислу, ближе се одрежују термини: криптобезбедност, криптозаштита, и безбедносна зона.

Приликом планирања и примене мера заштите ИКТ система треба се руководити начелима:

1) начело управљања ризиком – извор и ниво примене мера заснива се на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се створио, укључујући све врсте ванредних околности;
2) начело свеобухватне заштите – мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система;
3) начело стручности и добре праксе – мере се примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности;

4) начело свести и оспособљености – сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесни ризика и поседују одговарајућа знања и вештине.

У циљу остваривања сарадње и усклађености обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности, Влада је задужена да оснује *Тело за координацију послова информационе безбедности* као координационо тело Владе. У састав Тела улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретеријата Владе, Управе за заједничке послове републичких органа и представници Националног ЦЕРТ-а. Влада је донела *Одлуку о образовању Тела за координацију послова информационе безбедности*, 2016. године.

За наш предмет истраживања је од посебног значаја Члан 16 Закона, будући да одређује *финансијске институције као делове ИКТ система од посебног значаја*, услед чега се на њих примењују посебне мере заштите.

Поред финансијских институција, у ИКТ системе од посебног значаја спадају они који се користе: у органима јавне управе, за обраду нарочито осетљивих података о личности и у обављању делатности од општег интереса. Делатности од општег интереса су:

- производња, пренос и дистрибуција електричне енергије;
- производња и прерада угља;
- истраживање, производња, прерада, транспорт и дистрибуција нафте и природног и течног гаса;
- промет нафте и нафтних деривата; железничког, поштанског и ваздушног саобраћаја;
- електронска комуникација;
- издавање службеног гласила Републике Србије;
- управљање нуклеарним објектима;
- коришћење, управљање, заштита и унапређење добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја);
- производња, промет и превоз наоружања и војне опреме;
- управљање отпадом;
- комуналне делатности;
- здравствена заштита;
- услуге информационог друштва намењенњ другим пружаоцима услуга информационог друштва у циљу омогућавања пружања њихових услуга.

Влада је на предлог министарства задуженог за послове информационе безбедности донела *Уредбу о утврђивању Листе послова у областима у којима се обављају делатности од*

општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја, (2016.).

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, (2016.), одређује мере заштите ИКТ система од посебног значаја. Оператери су добили обавезу израде Акта о безбедности ИКТ система од посебног значаја, а обавеза је конретизована доношењем одговарајућег акта (*Уредба о ближем садржају акта о безбедности информационо-комуникацијског система од посебног значаја, начину провере и садржају извештаја о провери безбедносно-инфорамционог система од посебног значаја 2016.*)

Чланови 9 и 10 Закона регулишу питање поверавања активности у веи са ИКТ системом од посебног значаја трећим лицима. Под трећим лицем сматра се привредни субјект који је имовинским и управљачким односима повезан са оператером ИКТ система од посебног значаја.

Извештавање о инцидентима (Члан 11) регулисано је доношењем *Уредбе о поступку достављања података, листи, врстама и значају инцидента и поступку обавештавања о инцидентима у информационо-комуникацијским системима од посебног значаја (2016.)*.

Члан 12 се бави питањем међународне сарадње и одређује обаезу надлежног органа да остварује међународну сарадњу у области ИТК система – посебно да пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова:

- брзо расту или имају тенденцију да постану велики ризици;
- превазилазе или могу да превазиђу националне капацитете;
- могу да имају негативан утицај на више од једне државе.

Успостављање Националног центра за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ), Закон је прописао у Члановима 14 и 15.

Национални центар за превенцију безбедносних ризика у ИКТ системима Републике Србије основан је у оквиру Регулаторне агениције за телекомуникације и поштанске услуге.

Национални ЦЕРТ води евиденцију посебних ЦЕРТ-ова. Посебан ЦЕРТ је тим који обавља послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правнихи лица или области пословања и слично.

Надзор над радом Националног ЦЕРТ-а спроводи Надлежни орган, односно Министарство за трговину, туризам и телекомуникације.[267]

Национални ЦЕРТ посебно:

- прати стање о инцидентима на националном нивоу;
- пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима;

[267] Доступно на: https://www.ratel.rs/cyr/page/cyr-nacionalni-cert

- реагује по пријављеним или на други начин откривеним инцидентима, тако што пружа савете на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања;
- континуирано израђује анализе ризика и инцидената;
- подиже свест грађана, привредних субјеката и органа јавне власти о значају информационе безбедности, о ризицима и мерама заштите, укључујући спровођење кампања у циљз подизања те свести;
- води евиденцију посебних ЦЕРТ-ова.

Посебни ЦЕРТ-ови су регулисани Чланом 17 Закона. Услови за упис посебних ЦЕРТ-ова у евиденцију прописани су *Правилником о ближим условима за упис у Евиденцију посебних центара за превенцију безбедносних ризика у информационо-комуникацијским системима (2017.)*.

Закон регулише и проблематику криптобезбедности и заштите од компромитујућег електромангетног зрачења, као и делокруг послова о овлашћења инспекција за информациону безбедност (Чланови 28 и 29).

Инспекција за информациону безбедност врши инспекцијски надзор над применом закона и радом оператера ИКТ система од посебног значаја, осим самосталних оператера ИКТ система и ИКТ система за рад са тајним подацима, а у складу са законом којим се одређује инспекцијски надзор.

Законодавац је предвидео новчану казну у износу од 50.000,00 до 2.000.000,00 динара за правно лице, ако не донесе Акт о безбедности ИКТ система; не примени мере заштите одређене тим актом, не изврши проверу усклађености примењених мера и не поступи по налогу инспектора за информациону безбедност у остављеном року.

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

Интерни правни акти спадају у домен недржавног или аутономног права. Унутрашња правна регулатива представља механизам у области *менаџмента ризика*.

Предузећа на овај начин самостално уређују питања процене, превенције и контроле ризика која нису регулисана државним правним актима или примењују законске норме, прилагођавајући их специфичностима сопствене организације, структуре, делатности и система пословања. На тај начин унутрашњи правни акти могу да надокнаде недостатке спољне регулативе и могу да створе оптималан систем за спровођење законских обавеза. То

је процес инструментализације правних овлашћења организације за сврхе менаџмента кризе.[268]

Непостојање унутрашње нормативне регулативе може се окарактерисати као правни ризик.

Међународни стандарди и други документи углавном изостављају појам правног ризика, иако помињу овај термин, или га одређују описно или као подврсту друге категорије ризика.

Базелски комитет за надзор банака усвоји је, почев од 1988. године, три сета препорука – Базел 1, Базел 2 и Базел 3 – који се односе на оперативне и финансијксе ризике у пословању банака, о чему ћемо касније детаљније разматрати. Верзија Базел 2 (2004.) експлицитно помиње правне ризике, али их не дефинише, већ их само сврстава у категорију *оперативних ризика*.

Национални стандард за процену ризика у заштити лица, имовине и пословања (СРПС Ал2:003.2008.) је поставио критеријуме за идентификацију и оцену правних ризика, који испитују да ли у организацији постоји следеће:

- адекватна регулатива којом се смањује могућност одавања тајних података, пословних тајни, података о личности (укључујући нарочито осетљиве податке) и других штићених информација непозваном лицу или конкурентској организацији (комерцијална шпијунажа);
- адекватна регулатива којом се предвиђа радноправна одговорност лица због непоштовања интерних процедура у области безбедности лица, имовине и пословања које су проузроковале или могле да проузрокују негативне имовинске или неимовинске последице по корисника;
- адекватна регулатива и организација којом се смањује опасност од неадекватног мониторинга судских, управних и других спорова и поступака које предузеће води;
- адекватна регулатива којом се смањује могућност наступања пропуста у процесу обезбеђивања лица, имовине и пословања организације услед неадекватне интерне регулативе.

Задатак интерне правне регулативе у заштити података огледа се у предузимању одговарајућих нормативних мера након одговарајуће идентификације, класификације и систематизације препознатих ризика и њихове анализе и оцене.

Процена правних ризика одговара на следећа питања:

- да ли је предузеће усаглашено са законским захтевима у области заштите података;
- да ли непостојање или неадекватност законске регулативе поставља ризик по заштиту података података корпорације;
- да ли су интерни акти предузећа сачињени тако да предузеће оптимално користи законске механизме заштите.

[268] Г. Мандић, Н.Путник, М. Милошевић, op.cit., стр. 274.

У интерне акте правног лица убрајају се: статут, правилници, одлуке, пословници и други акти, као и процедуре и упутства.[269]

Значај интерне регулативе огледа се у заштити пословне тајне, јер ова материја јесте дефинисана законом и другим прописима, али је и остављен простор за организације да интерним актима ближе регулишу поједина питања, и на тај начин додатно се заштите у односу на изворе угрожавања у овом смислу. Такође, законска заштита може да се активира тек уколико је присутна интерна регулатива заштите пословне тајне.

Ефикасно регулисање пословне тајне може се постићи сетом унутрашњих прописа, али је треба и регулисати највишим интерним правним актом организације.

Средишњи део пирамиде у хијерархији интерних докумената чине одлуке и правилници, као општи правни акти којима се прецизира начин извршења неког механизма заштите, како смо претходно дали (Схема број 16: *Хијерархија нормативних докумената организације*).

Највиши степен конкретизације, у циљу операционализације дају процедуре и интерна упутства.[270]

Ми смо у поглављу о заштити информација, у делу о нормативној уређености, дали да су *Политике* кровни интерни документи којима се одређују начела поступања запослених у погледу заштите информација.[271]

Мишљења смо да разлике у називу интерних докумената, како смо то ми дали у наведеном поглављу, а руководили смо се међународном праксом у остваривању заштите информација, нису суштински различите од претходно изнетог, будући да је суштина концепта који дискутујемо у потреби да је у организацијама развијена интерна регулатива, са својим међусобним односима и принципима општости и конкретизације (појединачних) различитих питања у остваривању система заштите. Такође, у закључним разматрањима тог поглавља, определили смо се, у осврту на различиту терминологију у домаћој и међународној пракси, да ћемо у даљем раду користи ону терминологију, како нам то наводе наши извори истраживања.

[269] *Ibid*, стр. 278.
[270] *Ibid*, стр. 279.

[271] У пирамидалном моделу ми смо интерна документа дефинисали према следећем: Повеља (декларација) о безбедности (енгл: *Charter/Code of Conduct*); Политика безбедности (енгл: *Policy*); Безбедносни стандарди (енгл: *Standard*); Смернице из области безбедности (енгл: *Guideline*); Безбедносне процедуре (енгл: *Procedure*); Инструкције из области безбедности (енгл: *Instuction*) и Контролне листе, алати и слично (енгл: *Tool, Control, Baseline etc*)

2.1. Правилник о пословној тајни

Правилник о пословној тајни, представља средишни део у организацији интерних аката, и односи се на документ који разрађују сва питања у вези са поверљивим пословним информацијама и омогућава успешну заштиту организације. Намена овог документа јесте да одреди документа и информације које, у складу са законима и највишим правним актом правног лица, представља пословну тајну. Саопштавање овако одређених информација неовлашћеним лицима било би противно пословној политици правног лица и штетило би његовим пословним интересима и угледу.

Одговорност чувања пословне таје је на свим запосленима, односно на свим лицима која су по основу правног односа са правним лицем, на било који начин сазнали за документа и информације које представљају пословну тајну. Обавеза чувања пословне тајне не престаје престанком радног односа, односно уговорног односа за лица која су по таквом основу сарађивала са организацијом.

Важно је да сва лица (и запослени и пословни сарадници) буду упозната са Правилником и да након тога потпишу *Изјаву о чувању пословне тајне*.

Полазећи од праксе да се у пословном речнику у домаћој пракси, како смо до сада више пута истакли (оправадано или не) масовно користе термини на енглеском језику, напоњемо да се Изјава о чувању пословне тајне назива и: *Non-Disclosure Agreement (NDA), Confidetiality Agreement (CA), Confidental Disclosure Agreement (CDA), Proprietary Informaton Agreement (PIA) i Secrecy Agreement (SA).*

Садржај Правилника треба да се односи на: документа и информације које представљају пословну тајну; одређивање и означавање пословне тајне, укључујући поступак проглашења података за пословну тајну (уз одговарајућа овлашћења и дужности органа и запослених); упутство или методологију за процену ризика од неовлашћеног откривања, прибављања и саопштавања података проглашених за пословну тајну; начине руковања документима и информацијама које представљају пословну тајну; заштиту пословне тајне и повреду чувања пословне тајне.[272]

2.2. Правилник о приватности

Важна област за организације је и материја заштите података о личности. Законодавац не захтева да правно лице донесе интерне опште акте којима би регулисао прикупљање, чување и обраду података о личности, потребе заштите од социјалног инжењеринга и других облика компромитације и злоупотребе података о личности намећу овакву потребу.

[272] Више о садржају Правилника о пословној тајни: Мандић, Г., Путник, Н., Милошевић, М., *op cit.,* стр. 280. – 290.

С тим у вези, могуће је донети *Одлуку о поступку приликом прикупљања, обраде и евиденције података о личности (или Правилник о приватности)*. Овим документом се уређује начин поступања запослених приликом наведених радњи, у складу са прописима којима се утврђују услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују.

Препорука је да организација донесе *Политику заштите података о личности*, где се прецизира да организација врши обраду неопходних података оних лица која су дала пристанак за обраду.[273]

Надлежни орган одређује решењем лице задужено за координацију активности у погледу чувања, обраде и прикупљања података о личности и испуњавања законских обавеза, укључујући формирање и пријављивање збирки података о личности и предузимање организационо-техничких мера за заштиту података.[274]

Ради остваривања ове области заштите података, организације користе индустријске стандардне заштитне мере, као што су: физичка заштита простора (контрола приступа, против провални систем, *CCTV* и друго), заштиту информационе мреже, кадровску селекцију и техничка средства заштите (*firewall*, *password* и друго).

Важно је у Правилнику навести *законске обавезе руковаоца, будући да је он дужан да доставља Поверенику евиденцију о збирци података*, односно промене у евиденцији података, најкасније у року од петнаест дана од дана успостављања, односно промене, а обавештавања и евиденције у Централни регистар.

Примери евиденције које би ушле у збирку могу да обухватају и следеће:

- евиденција о запосленима;
- евиденција о уласку, кретању и боравку других лица у пословним објектима;
- евиденција о *ID* картицама за приступ, кретање и боравак у пословним зградама;
- евиденција о стручном образовању и усавршавању;
- евиденција о здравственом стању и повредама на раду;
- евиденција о поклонима;
- евиденција сачуваних снимака са *CCTV*-а;
- евиденција о зарадама, накнадама зарада и другим личним примањима;
- евиденција радног времена.

Посебну пажњу Правилник о приватности треба да посвети заштити нарочито осетљивих података о личности, где треба прописати да се пристанак за обраду нарочито осетљивих података даје у писаном облику (и да садржи: ознаку податка који се обрађује, сврху обраде и начин коришћења). Саставни део документа треба да буде Образац за прикупљање ових података.

[273] *Ibid*, стр. 290.
[274] *Ibid*

Полазећи од предмета нашег истрживања, за нас је (за заштиту информација у банкама и другим финансијским институцијама) од посебне важности превенција манипулисања личним подацима, од ЈМБГ броја грађанина до података о брачном стању, запослењу, висини месечних примања или неког сличног податка – посебно у доба глобалне информационе повезаности.

Подаци о личностима често су предмет напада који се врши неком од метода социјалног инжењеринга, што може представљати имовинску или репутациону штету организацији, одакле произилази и значај развијања нормативних механизама у заштити информација.

2.3. Безбедносна правила и процедуре

У досадашњем тексту већ смо напоменули важност конципирања безбедносне политике организације кроз изградњу нормативне основе остваривања послова безбедности. Архитектура безбедносних докумената, о чему смо такође изнели запажање о различитој пракси у међународној пракси и домаћим теоријским изворима, када је у питању номенклатура интерних докумената организације, подразумева да морају да се поштују правила која долазе из спољашњег окружења организације, а односи се на правне оквире окружења у којем организација послује. Са друге стране, интерни документи морају да одржавају ставове организације о одређеним питањима, и да следствено намени документа, одређују начине како ће организација да постигне циљеве за које се определила.

У таквим односима, као крајњи производ (условно речено, јер архитектура безбедносних докумената може да се посматра и одоздо према горе, од највећег степена конкретизације одређене области па до политика безбедности), јављају се правила, инструкције, процедуре, упутства, стандардизовани поступци и друга интерна документа организације у области безбедности.

Безбедносна правила престављају јасне смернице које одређују начин понашања свих запослених у функцији заштите одређених вредности ентитета.[275]

Начелно, безбедносна правила су условљена обликом и извором угрожавања организације, што је одређено у безбедносној политици. На основу усвојене политике доносе се безбедносна правила.

По утврђивању правила безбедности потребно их је уобличити у писани документ, упознати запослене са садржајем, урадити едукацију (тренинг), одредити и применити контролне активности за примену правила, одредити вредности које се прате као би мерили ефикасност спровођења утврђеног правила и – радити као континуирани процес евалуацију

[275] *Ibid*, стр. 337.

утврђених правила. Подсетимо, према нашим ставовима безбедност организације је процес, а не готов производ.

Опште је прихваћено да стил писања безбедносних докумената треба бити јасан и концизан за кориснике. У том смислу, неопходно је избегавати сувишне стручне и нејасне термине и треба тежити да текст буде не само разумљив него и прихватљив крајњем кориснику (за којег се и пишу правила, која се односе на све у организацији).

На пример, безбедносно правило може бити забрана коришћења флеш меморије на неким радним станицама. У пракси, када су у питању организације са осетљивим пословним информацијама (дакле подаци не морају бити нужно класификовани као пословне тајне), као што су банке и финансијске инстиуције, начелно се забрањује коришћење флеш меморије на свим радним станицама, а изузетно, и уз поштовање безбедносног принципа да се нека привилегија одобрава само оним запосленима којима је то неопходно ради обављања радног процеса (енгл: *need to do*), оваква привилегија се одобрава. Применом техничких мера ово правило се остварује блокадом *USB* портова, и у том смислу остваривање правила није спорно. Наш приступ је да овакав поступак јесте ефикасан (примена техничких мера), али да му недостаје развијање свести корисника због чега је он потребан (примена нетехничких мера).

Разлике у ова два приступа превазилази процес писања безбедносног документа, како смо претходно изнели, што у крајњем за резултат има да запослени примењују безбедносна правила као нешто што се подразумева.

Написана безбедносна правила подложна су ревизији и изменама, у зависности од околности које су довела до потребе одређивања правила.

Начин комуникације, о чему смо разматрали у поглављу о моделима могућег организовања послова безбедности у организацији, у оквиру овог рада, је једнако важан као и сам процес писања документа. Пожељно је да у процесу доношења безбедносних правила учествује цела организација, у мери у којој се та правила односе на њу. Овде није реч о консензусу у организацији, већ о томе да се пре доношења неког интерног акта са циљевима његовог доношења и принципима будућег функционисања упознају надлежни руководиоци који ће и бити задужени за спровођење договорених одредби.

У ту сврху препорука је да организациони део безбедности, са аспекта струке, састави радну верзију документа, коју даје на консултације руководиоцима надлежних пословних функција које ће бити укључена у реализацију овако дефинисаних правила, како би они доставили евентуалне примедбе и сугестије.

Безбедносне процедуре представљају унапред одређене, утврђене, успостављене и документоване методе и начине рада и поступак са којима су запослени упознати и по којима су обавезни да поступају.[276]

[276] *Ibid*, стр. 338. – 341.

Основна улога процедура је да операционализују претходно дефиниса безбедносна правила (која изнели смо већ, проистичу из безбеднсоних правила).

Процедура је детаљан документ који описује тачне акције које су неопходне за примену одређених сигурносних механизама, контрола или решења. У себ укључују све неопходне кораке у спровођењу одређених радњи и поступака, као и одговорност лица која их спроводе. Можемо рећи да су процедуре у суштини детаљне и прецизне инструкције о томе како је потребно сваки део радног процеса спровести правилно и комплетно.[277]

Форма писања овог документа може бити различита, у зависности од теме која се разматра, у зависности од претходно постојећег нормативног оквира уређености система безбедности организације, и посебно – у зависности од безбедносне културе организације и стања безбедносне свести запослених. У том смислу она може бити дата у форми алгоритма, писаног текста или комбиновано.

Мандић наводи да се процедуре, у односу на субјекте обезбеђења, могу посматрати двојако – у ширем и у ужем смислу.[278]

У ширем смислу, када је у питању сопротстављање социјалном инжењерингу, оне треба да омогуће следеће:

- спровођење правилног рада са класификованим документима;
- уништавање докумената која више немају употребну вредност;
- рад кадровске службе приликом запошљавања и по престанку рада запослених – процедуре приликом запошљавања и у случају престанка радног односа;
- физичко-техничку заштиту коју извршвају сви запослени;
- контролу приступа у зависности од категоризације простора;
- контролу безбедности простора правног ентитета приликом његовог напуштања провера да ли су закључана врата, провера сефа, укључивање ноћног светла, да ли је укључен систем против провале и друго);
- проверу идентитета лица без обзира да ли је контакт са њим директан или преко телефона;
- ненапуштање канцеларије и радног простора ако се у њему налази било које лице које ту није запослено;
- правилан рад са рачунаром са аспекта заштите од социјалног инжењеринга (креирање и замена шифре, рад са електронскмо поштом и коришћење рачунара у пословном јавном простору);
- пословне комуникације са тежиштем на заштити ифнормација и података

[277] *Ibid*

[278] Мандић, Ј. Г., *Систем обезбеђења и заштите правних лица,* Факултет безбедности, Универзитет у Београду, Београд, 2015. година, стр. 341.

- правилно одржавање хигијене рестриктивних просторија, у безбедносном смислу;
- мере приправности и поступања у случају сумње или откривања напада социјалним инжењерингом.

Процедуре у ширем смислу, саставни су део процедура процеса рада свих запослених (на пример, са аспекта заштите информација то би могла да буде процедура како се напушта радно место на крају радног времена, тзв. „политика чистих столова“, енгл: *Clean Desk Policy,* или – политка која одређује да запослени не могу поједине процесе рада, као што је улажење у неке рестриктивне просторе, да обављају самостално, енгл: *Four Eyes Principle* или *Two-man rule*). У банкакама се ови принципи односе, на пример, на *сакључарство* – принцип да каси са вредностима могу да приступе само двоје истовремено присутних запослених, са одговарајућим привилегијама, где на пример, један има кључ за механичко отварање касе, а други дигиталну шифру, или где обоје имају шифру (у зависности од модела браве), у сваком случају, обезбеђено је правилом да касу могу да отворе само двоје истовремено присутних запослених, по правилима и претходно додељеним привилегијама. Исти принцип може да се користи за друге радне процесе итд.

Са аспекта заштите информација, процедуре у ужем смислу биле би оне које се доносе како би одредиле неки процес који се одвија у пословној функцији безбедности организације или некој другој (на пример, процес издавања израде идентификационих картица запослених би одредио где се *ID* картице чувају, које мере заштите неовлашћеног приступа су примењене, ко је задужен за овај процес и у којим његовим деловима, на основу чега се разматра неки захтев – која су безбедносна правила, који су нивои привилегија који се могу доделити запосленом – која су безбедносна правила, како се захтев евидентира и обрађује, како се интерни идентификациони документ доставља запосленом, који је период важења документа, када се и како документ ставља привремено или стално ван функције, који је поступак када запосленом престаје радни однос, који је поступак када се против запосленог води дисциплински поступак или интерна истрага, који је поступак када запослени пријави губитак *ID* картице, који је механизам да се обезбеди правило да се идентификациона картица не користи неовлашћено, колико често се и на који начин проверавају додељене привилегије које картица подразумева, колико често се и на који начин проверава број присутних картица у систему контроле приступа, колико често и на који начин се проверава број „бланко“, издатихкартица, где се и на који начин чувају враћене ID картице, који је поступак уништавања ID картица и друго). Слично се може одредити процедуром коју доноси организациони део који штампа платне картице за клијенте, што је опет део који је препознат у међународном стандарду, а банкама остаје да га конретизују.[279]

[279] Усклађеност са Стандардима безбедности података у индустрији платних картица (*PCI DSS*) захтева од свих правних лица која чувају, обрађују или преносе податке власника картице, укључујући финансијске установе, трговце и пружаоце услуга, који редовно морају да демонстрирају дату усклађеност. Доступно на: https://rs.visa.com/partner-with-us/pci-dss-compliance-information.html#1

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

Слично као и нетехнички приступ у остваривању заштите информација, овај аспект заштите је, према нашем мишљењу, неоправдано запостављен у пракси.

Какве год мере организација да предузима, оне увек зависе, више пута је истакнуто до сада, од најслабије карике у ланцу система заштите, а то је човек – истовремено неко ко осмишљава и спроводи мере заштите и као неко ко истовремено представља непресушни извор угрожавања тог истог система.

Како ће се људи односити према прописаним мерама заштите зависи од више мера, организационих, нормативних, техничких, а пре свега зависи од стања свести о безбедности (енгл: *security awareness*) и безбедносне културе која је *спонтано прихваћена* у организацији.

Правни субјекти могу да утичу на понашање људи применом казнених мера, које се своде на страх запослених од ауторитета руководиоца, као и од страха од казни које следе у случају непридржавања у остваривања планираних мера. Овакав приступ у организовању мера заштите је заправо илузија у остваривању планираног нивоа безбедности, јер је понашање људи тада само тренутно и односи се на избегавање санкција.[280]

Једина исправна алтернатива оваквом приступу јесте постизање одређеног нивоа понашања запослених, где они разумеју значај информација и њене заштите, односно где су они свесни да њихови поступци, када нису у складу са планираним мерама, могу да угрозе виталне вредности организације у којој су ангажовани.

Безбедносна свест запослених и одговарајући едукативни садржаји који се спроводе (тренинзи) често се сврставају у исту врсту активности, јер се свест о неком феномену мења са сазнањима које човек има о томе, али не нужно. Образац – више знања доноси и већу безбедносну свест није увек успешан, јер се запостављају многи други аспекти о законитостима понашања људи у организацији. У том смислу, безбедносни тренинзи, могу да представљају нормативну меру организације у остваривању заштите информација, јер се ове активности планирају, раде се програми за подизање свести (интерни документи), израђују се одговарајући видео и други садржаји (постери, пригодне поруке путем електронске поште и друго), али остаје и да запослени промене вредносне ставове и своје понашање, као меру која је прихваћена и очекивана у њиховом радном окружењу – што остаје као питање за себе.

[280] Мандић, Г., Путник, Н., Милошевић, М., *op cit.*, стр. 342.

У поглављу где смо дали приказ неких научних радова који су релевантни за наш предмет истраживања, представили смо доста налаза која се односе на проблематику развоја безбедносне свести запослених. Можемо да истакнемо, као претежне ставове аутора, да безбедносну свест запослених карактерише следеће:

- заштита информација препознаје људе, њихово понашање, као најслабију карику у ланцу који чини тај систем (поред процеса и технологије);
- подршка менаџмента је кључна у спровођењу информационе безбедности;
- на свест запослених о информациној безбедности може да се утиче организацијом одговарајућих тренинга, који треба да су базирани на процени ризика за конкретну организацију;
- организациона култура је незаобилазни фактор у развоју безбедносне свести
- Шајн (*Edgar Schein*), одређује организациону културу као образац заједничких основних претпоставки на основу којих је група научила како да решава проблеме спољне адаптације и унутрашње интеграције, и образац који се може преносити новим члановима организације, као исправан начин перцепције, размишљања и осећања за исте потребе;
- неуспех повећања свести о информациноој безбедности је последица занемаривања организационе културе;
- потребно је повећати учешће запослених у одлучивању (у смислу позитивног утицања на њихову безбедносну свест уколико учествују и у формулисању циљева организације);
- Стандард ISO 17799 и друге препоруке дају препоруке најбоље праксе, где је једна од кључнихи активности увођење програма о развоју безбедносне свести у заштити информација. Није доречено како организовати тренинге, а у пракси је примећено да такви програми занемарују образовне принципе, што се усложњава чињеницом да програме за развој свести формирају углавном *IT* професионалци, који осим техничких знања (која нису спорна као неопходна), немају друга потребна знања (потребно је познавање: образовних принципа за образовање одраслих, разумевање контекста безбедности као феномена у пословном окружењу, садржај безбедности као пословне функције и друго);
- код прављења образовних програма у организацијама, за развој свести о безбедности, није циљ припремити полазнике за полагање формалног испита, или за даљи ниво формалног образовања, већ утицати на њихову свест;
- у теорији је у доброј мери развијен концепт промене корпоративне (организационе) културе, али је недовољно развијен процес промене супкултуре заштите информација. Начелно, мора се уважити: профил радне снаге, опис њихових послова, интерна организација рада, старосна и образовна структура, њихово радно искуство и друго;
- неке од препорука за организовање добрих програма за развој безбедносне свести су: сви запослени треба да су у прилици да успешно савладају тренинг, запослени треба да разумеју због чега су им потрена одређена знања и вештине, као и због чега треба да се понашају на одговарајући начин, материјале за учење треба прилагодити

стилу учења, полазници треба да су одговорни за своје учешће у тренинг програму и − полазници треба да добијају повратне информације о успешности обуке;
- теорија организационог учења није сама по себи довољна за промену безбедносне организационе културе, већ је потребно применити знања која долазе из менаџерских наука;
- покушај промене заједничких прећутних претпоставки, организационе односно безбедносне културе у организацији, ако није спроведен на одговарајући начин, може да резултира психолошком анксиозношћу међу запосленима

На крају, дали смо схему промене организационе културе (Схема број 4: *Организациона промена културе безбедности информација засноване на едукацији запослених*)[281], као допринос дискусији на који начин је овом проблему у остваривању заштите информација могуће приступити.

3. Нормативни оквир заштите информација у банкама и финансијским институцијама

У разматрањима о нормативном уређењу заштите информација, навели смо да Ранђеловић сагледава правну регулативу „компјутерског криминала", кроз правну регулативу у међународној заједници и кроз правну регулативу високотехнолошког криминала у Републици Србији. У том смислу он наводи активности које се обављају преко Организације уједињених нација, Организације за европску сарадњу и развој (ОЕЦД), Савета Европе и Европске уније, када је у питању међународни оквир. За сузбијање компјутерског криминала, када је у питању домаћа пракса, он наводи да је уређена *међународним конвенцијама, законским и подзаконским актима*, и наводи који су то правни акти.[282]

На овај начин, проблему заштите информација може да се приступа од општег нивоа (међународног нормативног оквира), посебног (закони, подзаконски акти, стандарди и друго) до појединачног нивоа (поједине гране привреде).

Претходно смо анализирали нормативни оквир у остваривању заштите информација у Републици Србији, такође, у поглављу о информационој безбедности изиели смо неке напомене о нормативне уређености ове области, али је потребно и да сагледамо како је нормативно уређена област заштите информација у банкама и финансијским институцијама у Републици Србији, у смислу сагледавања ове привредне гране на појединачном нивоу, како смо претходно навели.

[281] Niekerk, J.F., *op.cit.*, стр. 101.
[282] Ранђеловић, Д.: *Високотехнолошки криминал*, Криминалистичко-полицијска академија, ЈП „Службени гласник", Београд, 2013. година, стр. 309. – 336.

Домаћи банкарски сектор, не може се посматрати изоловано у односу на међународни, а и сама Република Србија се обавезала кроз принципе, стандарде и уговоре на одређене међународне обавезе да организује сопствене норме и прилагођава облике организације у различитим секторима своје одговорности, где сектор банкарства није изузетак.

Европском унија, у области заштите информација, како смо већ навели у овом раду, има развијен међународни оквир којим се уређује питање сајбер безбедности и приступа овом проблему са више аспеката: безбедносног, економског и политичког. До сада, највећи допринос је дала Евроспка агенција за безбедност мрежа и и информација (*ENISA*), чија је једна од улога да ради заједно са државама чланицама ЕУ и приватним сектором на развоју ове области.

У раду говоримо о заштити информација у банкама и финансијским институцијама, па је из тих разлога потребно да дамо ближе објашњење овог сектора, будући да, како ћемо касније видети, неке међународне обавезе које су важне за функционисање државе се остварују управу у банкарском сектору.

3.1. Појам и дефиниција банке

Пословање данашњих компанија не може се замислити без банкарског пословања и банака. Њихов живот и успех није могуће остваривати без послова платног промета којег банке обављају. Истовремено, банке су и извор финансирања развоја многих привредних субјеката – одакле све можемо да наслутимо колики значај имају банке за функционисање савремене друштвене заједенице.

Банкарство се бави и истраживањем улоге, значаја и пословања банака, као посебним институцијама финансијског и економског система земље. Оно има задатак да испитује и прати општа економска кретања која се испољавају функционисањем банака у банкарском систему. Другим речима, наука о банкарству проучава функције и улоге банкарског система, банкарско пословање, а нарочито односе, процесе и пословне транскације које се јављају по основу стварања и коришћења новца преко банака.[283]

Са аспекта историјског развоја, можемо рећи да се историја банкарства везује за историју новца. Појавом тржишне привреде настао је и новац, средство размене, одакле су савремени живот и пословање готово незамисливи без новца.[284]

Хаџић наводи[285] да је генеза банкарства проистекла из развоја банкарских послова, пре свих депозитног и кредитног посла, који одређују основну институционалну функцију банке као

[283] Џелетовић, М., Живковић, А., Бојовић, П.: *Банкарски менаџмент*, Чигоја штампа, Београд, 2008., стр. 7
[284] Ritter, S., Silver, W. L., Udell, G. E.: *Принципи новца, банкарства и финансијског тржишта*, УБС, Београд, 2009., стр.14
[285] Хаџић, М.: *Банкарство*, Универзитет Сингидунум, Београд, 2013., стр. 3

новчаног предузећа. Кредитни, мењачки и заложни послови постојали су већ у старом веку код Сумера, Асираца, у Вавилону, на Кипру, код Египћана и Грка.[286]

У старом Риму је дошло до административног регулисања финансијских институција и праксе. Римски банкари имали су назив *argentarius* – лице које се бави примањем депозита и улога, давањем зајмова и посредовањем у новчаном промету.[287]

У раном средњем веку карактеристичан је развој мењачких послова, јер је велики број владара совао сопствени новац, као и појава „кварења новца" (одступањем било у тежини, било у квалитету метала од којих је новац израђен). Тако је, на пример, у Енглеској сребрни пени 1300. године тежио 22 грама, а 1364. године свега 12 грама.[288]

Полазећи од предмета нашег истраживања, ми смо пронашли податак да је Цар Душан, 168. чланом свог Законика[289], забранио било коме, ко није добио дозволу, да кује новац. Цар изричито наређује да се новац може ковати само у градовима које је за ту сврху он одредио.[290] На овај начин је жеља била да се држава заштити од два зла: појединачне злоупотребе златара који би ковали новац без његове дозволе и – од узурпације права ковања новца од стране појединих представника повлашћених сталежа. На овај начин, Цар Душан је постао суверена монетарна власт. Иза члана 168. Законика стајала је филозофија европских сталешких монархија: „ Један владар, једно право и једна монета у читавом краљевству".[291]

Иначе, Цар душан је у Законику предвидео смртну казну за тајно ковање новца (али се та казна односила на златаре који кују новац, а не на властелине који би издавале овакве наребе – будући да се Цар на овај начин није хтео да замера (моћној) властели.[292]

Пре Цара душана, Сефан Драгутин (владао од 1276. – 1282. године) засновао новчани систем на *тешком сребрном грошу,* уведеном у Венецији почетком 13. века. Тада је Србија постала значајни произвођач извозник сребра. У Жичкој повељи, око 1220. године, казне су биле изказане у коњима и воловима, а у повељама краља Милутина (владао од 1282. – 1321.) оне су биле одређене у новцу, чак и за сељаке, са изузетком Влаха који су традиционално

[286] Хаџић наводи да је Вавилонски краљ Хамураби (1792. – 1750. године п.н.е.) инспирисан Шамашом, богом сунца, донео закон т.ј. кодекс о банкарству, који се сматра првим банкарским кодексом, којим је банкарство прешло из верске у трговачку делатност. Место „бога банкара" заузимају бројни банкари, свештеници и велепоседници, који напуштају храмове и отпочињу праву банкарску трговину. Овај кодекс је био темељ целог правног система тог подручја и једини до појаве римских закона. Он прецизира банкарске послове као што су: зајам, камата, деопозит о роби, уговор о комисиону. Кодекс је такође говорио о зеленашењу, тако што су сви уговори о зајму подлегали одобрењу краљевог службеника. *Ibid,* стр. 3

[287] Хаџић, М, *op. cit*., стр. 4

[288] *Ibid*

[289] Душанов законик је донет на Вазнесење Господње, 21. маја 1349. године у Скопљу, на сабору властеле и црквених великодостојника.

[290] Више о томе: Селаковић, М. Н.: *Душанов законик и правни трансплантии*, упоредно-правна студија, Катедра за правну историју, Правни факултет, Универзитет у Београду, 2007.

[291] Више о томе: http://www.novosti.rs/dodatni_sadrzaj/clanci.119.html:303780-Car-Dusan---guverner

[292] *Ibid*

били сточари[293]. Први помен српског новца датира из 1277. године у Дубровачком цариснком статуту у одредби о таксама за извоз робе, где се спомињу *брсковски динари*[294], цењени новац тог времена. У Венецији, српски новац је био познат под именом „динари краља Рашке“ и први пут се помињу 1282. године у уредби којом се забрањује оптицај српских динара. Од 1292. године за новац са овог подручја се користи термин „рашки динари“. Поново се спомињу 1303. године у уредби у којој дубровачка влада да се новац „Рашке из Брскова и осталих крајева Србије забрани због умножавања и фалсификата у оптицају“. Око 1305. године, српски динари су служили као легално средство плаћања у Болоњи и били једна од основних новчаних јединица. Краљ Милутин је увео контролу ковања (због квалитета), па су се на динарима нашле ознаке које су представљале потпис одговорних лица. Овакав манир је потрајао све до раздобља цара Душана.

Ћелетовић, Живковић и Бојовић наводе да банкарство, као научна дисциплина, развило у другој половини XIX века. Банкари су се тада оспособљавали за успешно вођење банкарских послова, водећи рачуна о кредитном покрићу, ликвидности, пословном угледу и сл.[295]

Ови аутори сматрају да савремена схватања посматрају банку као специфично предузеће које послује новцем, због чега је његов друштвени значај већи у односу на друга „обична“ предузећа. Осим овог приступа („микроекономског“), банкарско пословање се третира као целина економских, финансијских и монетарних мера, којима се банкарски систем ставља у функцију учувања стабилности националне валуте, снабдевање потребном количином новца и кредита, ефикасног платног промета и др. (макроекономски приступ).[296]

Појам „банка“ потиче од латинске речи „banco“ која означава клупу (тезгу, у данашњем смислу шалтер), постављену на улици, тргу, вашару или сајму, на којој се вршила размена различитих облика и врста новца, као и новчане трансакције наплате и плаћања у веи са обављеним трговинским прометом.[297]

Хаџић, сматра да лингвистика и етимологија указују да је реч банка (италијански *banco*, француски *banque,* немачки и енглески *bank*), коришћена током више од 20 векова постојања у значењу „клупа“ или „пулт за замену новца“. Банка се може сматрати пословном јединицом – предузећем које обезбеђује банкарске услуге у профитне сврхе. У зависности од различитих услова у којима се банкарство развијало у појединим земљама,

[293] Краљ Милутин је произвео имитацију венецијанског сребрног новчића на Новом Брду у Призрену, који су садржали једну седмину или осниму сребра који је имао оригинални новчић. Венеција је забранила лажни новац, а песник Данте је Краљевину Рашку и краља Милутина у својој „Божанственој комедији“ означио као преваранта и доделио му место у паклу. Извор: *Ibid*

[294] Брсковска тврђава (звана и Градина) смештена је шест километара источно од данашњег Мојковца у Црној Гори и представља трвђаву из које је контролисана околина, у којој су се налазио комплекс рударско-трговачког насеља и где се ковао сребрни новац, који је преко венецијанских трговаца био цењен у Италији тог доба.

[295] Ћелетовић, М., Живковић, А., Бојовић, П., *op.cit.*, стр. 7

[296] *Ibid*

[297] *Ibid*

јавиле су се и разне дефиниције банака. У Енглеској се сматра да је основна карактеристика банака новчана емисија, у Француској посредовање у одобравању кредита, док је у Немачкој њихово учешће на берзама и бављење новчаним шпекулацијама. Банка је новчано предузеће и кредитна установа чији су основни послови депозитни, кредитни и послови платног промета. Банка такође може да се дефинише у смислу:

- економских функција – банке обављају трансфер средстава од штедиша ка зајмопривцима (финансијско посредовање) и плаћања за робе и услуге које су прометоване;
- услуга која пружа клијентима – банке пружају велики број услуга клијентима од одовравања зајмова компанијама, физичким лицима и државама, трговања хартијама од вредности (ХОВ), организовања и гарантовања емисија ХОВ, заштите осигурања, планирања финансија, управљања пензионим системима, до саветодавних услуга компанијама;
- правне основе постојања – банка је најпре (крајем XIX века у САД) дефинисана као било која компанија која пружа услуге депоновања средстава и одобрава зајмове, а скорије Савезна Корпорација за осигуранње депозита САД (*FDIC*) банку је дефинисала као било коју институцију која може да се пријави за осигурање депозита које је њеној надлежности.

Џелетовић, Живковић и Бојовић износе став да не постоји јединствена дефиниција банке. Они су мишљења да је то због тога што банкарски теоретичари имали у виду њену специфичност, па су је третирали као институцију или установу која обавља одређене функције, тј. појам банке су третирали са функционалног аспекта. Сходно томе, банка се сматра предузећем чије су функције резултат друштвене поделе рада. За разлику од других предузећа, банка је посредничко предузеће које мобилише и концентрише слободне финансијске ресурсе (најчешће у виду депозита) и врши њихову алокацију (најчешће у виду кредита). Банка финансијски посредује између финансијски дефицитарних сектора и трансактора. При томе, желећи да максимизира сопствену добит, банка оптимизира алокацију финансијских ресурса.

Касније, развојем трговине, банке се дефинишу као институције које су носиоци платног жиро промета. Настанком и развојем индустрије и спољне трговине, банке се дефинишу као кредитне институције.

Такође, и организациона теорија је оставила трага на покушају дефинисању појма банка. Тако се банке гтретирају као предузећа која имају за циљ максимизацију профита на уложени капитал власника. Да би то постигла, банка користи организационе иновације.[298]

Ови аутори износе мишљење да савремене теорије имају за основ теорију јавног карактера банке. Јавни карактер банке подразумева њен допринос стабилности националног финансијског система.

[298] *Ibid,* стр. 8

Полазећи од свега наведеног, Џелетовић, Живковић и Бојовић изводе закључак да је банка специфичан привредни и тржишни субјект, која, на бази пренетих овлашћења и поверавања, посредује у трансферисању туђих средстава (пре свега на кредитној основи), обављајући све новчане, депозитне и кредитне трансакције између финансијски суфицитарних и финанијски дефицитарних трансактора, вршећи при томе секундарну емисију новца уз испољавање високог степена професионалности, организованости и адаптираности на промене у друштевно-економском окружењу, што доприноси максимализацији сопствене микроекономије и оптимизације коришћења финансијских средстава у макроекономији.

Како би овако сложену дефиницију прегледније приказали, сами ауутори предлажу да се она расчлани, тако да се уједно приказују и карактеристике банке, на основу чега можемо закључити да је банка:

- самостални привредни и тржишни субјект;
- предузеће *sui generis;*[299]
- засновано на пренетим овлашћењима и поверењу;
- посредничка институција у трансферисању средстава између финансијски суфицитарних и финанијски дефицитарних трансактора;
- институција која обавља све новчане, депозитне и кредитне трансакције својих коминтената;
- иснтитуција која обавља своје функције професионално, огранизовано и адаптирано;
- својим пословањем унапређује микро и макроекономске аспекте банкарства.

Банке су институције које не функционишу самостално и оквиру финансијског система, наводи Хаџић.[300]

Он наводи да се финансијске институције дефинишу као поредници у трансферу средстава између дефицитарних и суфицитарних трансактора. Према овом аутору, финансијски посредници се сврставају у три основна типа:

- кредитне институције;
- институционални инвеститори;
- берзански посредници.

Основна карактеристика кредитних институција је да она пласирају средства претежно у облику кредита. Зависно од тога како формирају финансијски потенцијал – на бази депозита или на неки други начин, разликују се депозитне и недепозитне кредитне институције. Банке и штедионице спадају у депозитне кредитне институције. Финансијске компаније спадају у недепозтине кредитне институције.

[299] *Sui generis* – новолатински израз који значи да је нешто јединствено по својим карактеристикама
[300] Погледати више: Хаџић, М., op.cit., стр. 8

Институционални инвеститори су финансијске институције које пласман срестава врше улагањем у хартије од вредности (ХОВ). У ову групу финансијских посредника спадају пензиони фондови, осигуравајућа друштва и инвестициони фондови.

3.2. Класификација банака

Полазећи од претходно изнете класификације финансијских посредника, можемо рећи да у оквиру бројних финансијских институција у свим финансијским системима, банкама припада примарна улога.

Џелетовић и остали аутори износе[301] да у литератури не постоје јединствени критеријуми за поделу банака. Због тога се користи више критеријума, који се међусобно употпуњују. Најчешћи критеријуми су:

- рочност послова (комерцијалне банке – краткорочни послови; инвестиционе банке – дугорочни послови);
- привредна област из које потичу оснивачи банке (трговачке банке, спољнотрговинске банке, пољопривредне банке, индустријске банке);
- величини територије које покрива банка (општинска, регионална, национална банка – у случају федералних држава).

Најстарије банке биле су универзалног карактера, у смислу да су за своје коминтенте обављале све врсте банкарских послова. Развој индустрије и трговине доводи до специјализације у банкарству. То је дало доминантну улогу критеријуму (за врсте банака) који уважава врсту извора, природу средстава и начин њихове употребе од стране банке, уз постојање међузависности између врсте средстава и њиховог пласмана. Имајући у виду овај критеријум, уобичајена је подала банака на:

- централне или емисионе банке;
- пословне банке;
- комерцијалне (депозитне) банке;
- инвестиционе банке;
- универзалне банке;
- остале банке.

Централне или емисионе банке су оне на које држава преноси права и овлашћења у домену вођења емисионе, кредитно-монетерне, девизне политике и регулисања новчане масе.[302]

Пословне банке се заснивају на сопственим финанијским средствима, због чега код њих доминирају сопствени послови. Ове банке могу бити власници или сувласници многих

[301] Џелетовић, М., Живковић, А., Бојовић, П., *op.cit.*, стр. 7
[302] Хаџић, М., *op.cit.*, стр. 11

предузећа преко чијег профита увећавају сопствени капитал. Организују се као акционарска друштва која обављају краткорочне и дугорочне банкарске послове. У домаћој пракси овај назив се не користи адекватно, јер су наше пословне банке у суштини универзалне.[303]

Комерцијалне (депозитне) банке су оне код којих је примарни посао прибављање средстава из депозита и улога на штедњу.[304]

Инвестиционе банке се разликују од комерцијалних јер мобилишу средства најмање на средњи, а најшеће на дуги рок. Најстарији облик инвестиционих банака јесу хипотекарне банке. Ове банке своје пласмане обезбеђују хипотеком, којом се блокира право продаје непокретности дужника до истека кредита.

Треба напоменути да комерцијалне и инвестиционе банке имају све више сличности.

Универзалне банке су први организациони облик банака. Ове банке нуде читав низ финансијских услуга. Џелетовић и остали наводе да „у теорији постоје значајне дилеме о „универзалности“ банака. Између осталог, да ли универзулане банке повећавају ризик финансијске нестабилности, које банке (да ли универзалне или специјализоване) доприносе повећању економског развоја, да ли универзалне банке повећавају капитал, колико универзалне банке истискују друге финансијске институције, стварају концентрацију моћи и др.“[305]

3.3. Народна банка Србије (НБС)

Законом о Народној банци Србије утврђено је она централна банка Републике Србије и да обавља функције утрвђене овим законом. Народна Банка Србије је самостална и независна у обављању функција утрвђених законом, подлеже надзору Народне скупштине и њој одговара за свој рад (Закон о Народној банци Србије, 2015, члан 2, ставови 1 и 2).

Самосталност се огледа у одредби да Народна банка Србије, органи Народне банке Србије и чланови ових органа у обављању својих функција не примају нити траже упутства од државних органа и организација, као ни од других лица (Закон о Народној банци Србије, 2015, члан 2, став 3). Државни органи и организације, као ни друга лица, не могу угрожавати самосталност и независност Народне банке Србије, нити могу вршити утицај на Народну банку Србије, органе Народне банке Србије и чланове ових органа у обављању њихових функција (Закон о Народној банци Србије, 2015, члан 2, став 4).

Џелетовић, Живковић и Бојовић[306] наводе да је Народна банка Србије централна банка Републике Србије која је самостална и независна у обављању функција и за свој рад одговорна је Народној скупштини Републике Србије а у обављању совјих функција, неће

[303] Више о томе: Џелетовић, М., Живковић, А., Бојовић, П., *op.cit.*, стр. 12
[304] М. Хаџић, *Ibid*
[305] Џелетовић, М., Живковић, А., Бојовић, П., *op.cit, op.cit.*, стр. 14
[306] Џелетовић, М., Живковић, А., Бојовић, П., *op.cit.*, стр. 41

пиримити нити тражити упутства од државних органа и других лица. НБС, у извршвању својих функција, сарађује са Владом и другим државним органима и, у овкиру своје надлежности, предузима мере за унапређење те сарадње. За обавезе Народне банке Србије јемчи Република Србија.

У литератури нема неслагања око дефиниције НБС и њене улоге. Тако Хаџић наводи да је она централна (емисиона) банка Републике Србије и за њене обавезе јемчи Република. Она је самостална и независна у вођењу монетарне, кредитне, каматне и девизне политике. По концепцији организовања НБС је јединствена централна банка. У погледу својине капитал НБС је у власништву Републике Србије. НБС има право предлагања закона и других општих прописа из области монетарно – кредитног и девизног система и политике. За свој рад одговара Народној скупштини. Основна циљна фунцкија НБС је стабилност цена, при чему су у Закону такође набројани пораст производње и запослености, остваривање стопе привредног раста и остваривање платно – билансних циљева. [307]

Функције НБС су (Закон о Народној банци Србије, 2015, члан 4):

1) утврђује и спроводи монетарну и девизну политику;
2) управља девизним резервама;
3) утврђује и спроводи, у оквиру своје надлежности, активности и мере ради очувања и јачања стабилности финансијског система;
4) издаје новчанице и ковани новац и управља токовима готовине;
5) уређује, контролише и унапређује несметано функционисање платног промета у земљи и са иностранством, у складу са законом;
6) издаје и одузима банкама дозволе за рад, врши контролу бонитета и законитости пословања банака и обавља друге послове, у складу са законом којим се уређују банке;
7) издаје и одузима дозволе за обављање делатности осигурањам, врши контролу ове делатности, односно надзор над њеним обављањем, издаје и одузима овлашћења за обављање појединих послова из делатности осигурања и обавља друге послове, у складу са законом којим се уређује осигурање;
8) издаје и одузима дозволе за обављање послова финансијског лизинга, врши надзор над обављањем ових послова и обавља друге послове, у складу са законом којим се уређује финансијски лизинг;
9) издаје и одузима друштвима за управљање добровољним пензијским фондовима дозволе за рад и дозволе за управљање тим фондовима, врши надзор на овом делатношћу и обавља друге послове, у складу са законом којим се уређују добровољни пензијски фондови;
10) издаје и одузима платним институцијама дозволе за пружање платних услуга, а институцијама електронског новца дозволе за издавање електронског новца, врши надзор над пружањем платних услуга и издавањем електронског новца, а обавља и друге послове, у складу са законом којим се уређују платне услуге;

[307] Хаџић, М., *op.cit*., стр. 95

11) обавља послове заштите права и интереса корисника услуга који пружају банке, друштва за осигурање, даваоци финансијског лизинга, друштва за управљање добровољним пензијским фондовима, пружаоци платних услуга и издаваоци електронског новца у складу са законом;
12) утврђује испуњеност услова за покретање поступака реструктуирања банака, односно чланова банкарске групе и спроводи ове поступке, одлучује о инструментима и мерама које ће се предузети у реструктуирању и обавља друге послове у вези с реструктуирањем банака, у складу са законом којим се уређују банке;
13) издаје и одузима оператерима платног система дозволе за рад овог система, врши надзор над њиховим пословањем и обавља друге послове, у складу са законм којим се уређују платне услуге;
14) обавља законом, односно уговором утврђене послове за Републику Србију не угрожавајући притом самосталност и независност из члана 2. овог закона;
15) обавља друге послове из своје надлежности, у складу са законом

Полазећи од предмета нашег истраживања, овом приликом би нагласили *контролну функцију НБС*, будући да она издаје и одузима дозволе за рад, врши контролу бонитета и законитости пословања банака и других финансијских организација и предузима друге мере у складу са законом којим се уређује пословање банака и других финансијских организација.

„Народна банка Србије доноси прописе којима се утврђују стандарди банкарског пословања. НБС има право увида у пословне књиге и другу документацију банака и других финансијских организација, као и правних лица која су с банком, односно другом финансијском организацијом која је предмет контроле повезана имовинском, управљачим или пословним односима. НБС сарађује са страним институцијама надлежним за контролу пословања банака и домаћим органима и институцијама надлежним за надзор у области финансијског пословања, у циљу унапређења контролне функције НБС. НБС може да размењује податке прибављене у обављању контролне фунцкије са страним и домаћим органима и институцијама.“[308]

Неки од докумената који се у ширем или ужем смислу односе на област заштите информација у банкама и финансијским институцијама, а које је донела НБС су:

– *Одлука о минималним стандардима управљања информационим системом финансијске институције*, будући да овај акт утврђује миминалне стандарде и услове стабилног и сигурног пословања који се односе на управљање информационим системима у банкама, друштвима за осигурање, даваоцима финансијског лизинга и друштивма за управљање добровољним пензијским фондовима (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2019, члан 1, став 1).

[308] Џелетовић, М., Живковић, А., Бојовић, П., *op.cit,* стр. 48

- *Одлука о системима управљања и унутрашњих контрола платних институција и институција електронског новца и о заштити новчаних средстава корисника платних услуга и ималаца електронског новца*, будући да се овде, између осталог, дефинише обавеза институција да успоставе, одржавају и унапређују поуздане, ефикасне и свеобухватне системе управљања и унутрашњих контрола који обезбеђују одговорно и поуздано управљање институцијом (Одлука о системима управљања и унутрашњих контрола платних институција и институција електронског новца и о заштити новчаних средстава корисника платних услуга и ималаца електронског новца, 2019, члан 2, став 1).
- *Одлуку о управљању ризицима банке*, јер се овим актом прописују ближи услови и начин идентификације, мерења и процене ризика којима је банка изложена у свом пословању, осим ризика усклађености пословања, као и управљање тим ризицима, укључујући и начин израчунавања појединих показатеља пословања банке у вези са управљањем ризицима и ограничења који се односе на ризике. Посебну пажњу обратићемо ризицима које овај акт третира, односно посебно оперативном ризику, полазећи од његове природе и значаја који има не само на пословање банака, већ и значај који има за наш предмет истраживања (Одлуку о управљању ризицима банке, 2017, члан 1, став 1 и члан 2, тачка 8).
- *Упитник о информационом систему финансијске институције за 2018. годину*[309], будући да су овом анкетом обухваћене банке, друштва за осигурање, друштва за управљање добровољним пензијским фондовима и даваоци финансијског лизинга, а третира области: управљања информационим системом; управљање ризиком информационог система и ревизија информационог система; развој и одржавање информацоног система; безбедност информационог система и – континуитет пословања и опоравак активности у случају катастрофе.

3.4. Управљачка структура банке

Питање управљачке структуре банке је од значаја за предмет нашег истраживања, будући да се оваквим дефинисањем посредно утиче и на питање организације безбедносног сектора у оквиру финансијске институције.

У том смислу, за анализу управљачког процеса у банци значајно је сагледати функције Скупштине банке, Управног и Извршпног одбора банке, као и других одбора.

Скупштина банке је састављена од акционара банке, а они своје право гласа остварују непсоредно или преко својих представника. Статутом се акционарима који имају 1% или више акција с правом гласа не може онемогућити непосредно вршење права гласа.[310] Не

[309] https://www.nbs.rs/internet/cirilica/scripts/showContent.html?id=13339&konverzija=no
[310] Целетовић, М., Живковић, А., Бојовић, П., *op.cit,* стр. 55

разматрајући посебно конкретна задужења овог органа, напоменућемо да Скупштина доноси статут и доноси измене и допуне оснивачког акта и статута.

„Управни одбор има најмање пет чаланова, укључујући и председника. Најмање 1⁄3 чланова Управног одбора банке морају бити лица независна од банке, у смислу да немају директно или индиректно власништво ни у банци, ни у члану банкарске групе у којој је та банка. Чланови Управног одбора банке морају имати добру пословну репутацију и одговарајуће квалификације, које прописује НБС. Најмање три члана Управног одбора морају имати искуство из области финансија. Најмање један члан Управног одбора мора имати активно знање српског језика и имати пребивалиште на територији Републике Србије".[311] Од значаја за предмет нашег истраживања је да Управни одбор, између осталих функција: бира и разрешава председника и чланове Извршног одбора банке; врши надзор над радом Извршног одбора банке; успоставља систем унутрашње контроле и врши надзор над њеном ефикасношћу; усваја програм и план унутрашње ревизије и методологију њеног рада и – чему ми дајемо посебан значај због предмета нашег истраживања – утврђује унутрашњу организацију, односно организациону структуру банке која обезбеђује поделу овлашћења, дужности и одговорности запослених, на начин којим се спречава сукоб интереса и обезбеђује транспарентан и документован процес доношења и спровођења одлука.[312]

Извршни одбор банке – ИО (engl: *Executive board*), је колективни орган управљања банком. Чине га најмање два члана, укључујући и председника, који заступа и представља банку. У случају предузимања правних радњи, председник је дужан да обезбеди потпис још једног члана ИО. Чланови ИО су у радном односу, а да би имали тај статус морају имати добру пословну репутацију и потребну квалификацију. Најмање један члан ИО мора активно да говори српски језик и да има пребивалиште на територији Републике Србије, а остали чланови ИО морају имати боравиште на територији Републике Србије. Овај орган, према Закону о банкама има делокруг рада, наводећи према значају за наш предмет истраживања (Закон о банкама, 2015, члан 76, став 3, чланови 1 до 14):

- извршава одлуке банке и управног одбора банке;
- предлаже управном одбору пословну политику и стратегију банке, као и стратегију и политику за управљање ризицима и стратегију управљања капиталом банке;
- спроводи пословну политику и стратегију банке доношењем одговарајућих пословних одлука;
- спроводи стратегију и политике за управљање ризицима и стратегију управљања капиталом банке усвајањем процедура за управљање ризицима, односно за идентификовање, мерење и процена ризика, и обезбеђивањем њихове примене и извештава управни одбор банке у вези с тим активностима;
- анализира систем управљања ризицима и најмање тромесечно извештава управни одбор банке о нивоу изложености ризицима и управљању ризицима;

[311] *Ibid*, стр. 57
[312] *Ibid*, стр. 57 - 58

- обезбеђује сигурност и редовно праћење система информационе технологије и трезорско пословање банке;
- обезбеђује да сви запослени буду упознати с прописима и другим актима банке којима се уређују њихове радне обавезе;
- одлучује о свим питањима која нису у надлежности скупштине и управног одбора банке.

На овом месту би још једном истакли, у вези са организационим и нормативним уређењем заштите информација да је Извршни одбор орган који је према Закону о банкама *одговоран за праћење и мерење ризика (дакле и оперативног ризика), а посебно обезбеђује сигурност и редовно праћење система информационе технологије и трезорског пословања банке.*

Према Закону о банкама, банка је дужна да образује: одбор за праћење пословања банке (одбор за ревизију); кредитни одбор и одбор за управљање активом и пасивом (Закон о банкама, 2015, члан 79, став 1). Од значаја за предмет истраживања овог рада је и да банка може образовати и друге одборе (Закон о банкама, 2015, члан 79, став 2).

> „Један од најчешћих је Одбор за информатичке технологије (*IT*), који сачињавају чланови менаџмент тима, тј. Чланови ИО, руководилац сектора (одељења, службе) за *IT*, руководиоци сектора (одељења) за послове са становништвом, за кредите и инвестиције, за послове са иностранством, рачуноводства, за средства и ликвидност и директори главних филијала. Ово тело одлучује о:
>
> - дефинисању стратегије развоја *IT*;
> - доношењу развојних планова *IT* , њиховој реализацији и мерама;
> - инвестицијама у *IT*;
> - дефинисању супсидијара;
> - праћење примене јединственог инфо система *IT* у филијама.
>
> Контрола банкарског пословања врши се прво, од стране државне институције надлежне за то, а најчешће се ради о централној банци и друго, у самим банкама. Чланови ИО одговорни су за вршење унутрашње контроле над пословањем банке на свим нивоима. Одбор за праћење пословања банке и унутрашња ревизија банке врше контролу правилности рада банке и екикасности функционисања система унутрашње контроле. Банке је дужна да поступке система унутрашње контроле уреди и спроводи на начин који омогућава континуирано праћење и мерење свих врста ризика. Банка је такође дужна да систем унутрашње контроле развија на начин који омогућава благовремену процену ризика. Народна банка Србије прописује ближе услове и начин уређења и спровођења система унутрашње контроле у банкама. Контролу пословања пословних банака врше саме банке у посебно организованом одељењу за ревизију и контролу пословања банке су у складу са

Законом о банкама дужне да образују организационе јединице за контролу усклађености пословања банке и унутрашњу ревизију.“ [313]

Улога ових организационих јединица, наше је мишљење, логички и суштински је повезана и са остваривањем система безбедности у банкама, будући да у практичном остваривању банкарских послова свако одступање од планираног начина рада може да провоцира ескалацију било које групе ризика, посебно оперативних, одакле имамо намеру да ове организационе јединице посматрамо не само као законски обавезне функције у банкама, већ да их у ширем контексту доведемо у везу са остваривањем концепта безбедности у банкама.

3.5. Организациона јединица за контролу усклађености банке

(енгл: *Compliance Unit*)

Утемељена је Законом о банкама којим су одређени делокруг послова контроле, самосталност у раду и друго.

Одлука о начину и условима идентификације и праћења ризика усклађености пословања банке и управљање тим ризиком (Службени гласник РС, број 86/2007 и 89/2007), представља подзаконски акт који је на снази од 1. октобра 2007. године.

Законом се *ризик усклађености пословања банке сегментира као ризик од санкција регулаторних тела, финансијских губитака и репутациони ризик*. Одлуком се формулише да ризик усклађености пословања банке настаје као последица пропуштања усклађивања пословања са законом и другим прописом, стандардима пословања, процедурама о спречавању прања новца и финансирања тероризма, као и са другим актима којима се уређује пословање банака.[314]

Послови ове пословне функције обухватају:

- радње и мере у области спречавања прања новца и финансирања тероризма;
- заштиту клијената (права корисника финансијских услуга);
- поштовање банкарске тајне;
- конфликт интереса (правила управљања код процене постојања конфликта интереса);
- кодекс понашања унутар банке;
- кодекс понашања у продаји, трговини и маркетингу банкарских услуга (производа);
- правила везана за развој постојећих и одобравање нових услуга;
- злоупотребу тржишта и привилегованих информација које проистичу из посебних овлашћења.

[313] Хаџић, М., *op.cit*., стр. 125-126
[314] Бисић, В.: *Комплајанс, којим путем даље*, стручни чланак, Банкарство, 2018., vol. 47, бр. 4

Уколико се погледају међународни стандарди *compliance* фукције, које примењују „стране“ банке у Републици Србији, препознаје се другачији приступ у одабирању приоритета. Тако према *(Federal Sentencing Guidelines for Organizations - Effective Compliance and Ethics Program − FSGO)*, кључна начела за ефективни програм усклађености су:

- успостављање такве организације која ће са дужно пажњом спречавати и откривати криминално понашање;
- успостављање организације која ће промовисати културу која подстиче етичко понашање и поштовање закона.

Ова начела се разрађују кроз следеће елементе комплајанс матрице:

- успостављање политика и стандарда пословног и етичког понашања;
- успостављање верификације и надзора, те континуираног тестирања и контроле ради откривања криминалног понашања;
- промовисање културе *Ton at the Top*, као израз успостављања највиших етичких стандарда у врху организације, с циљем превенције превара и друге неетичке праксе;
- промовисање отворене линије комуникације за поверљиве информације, укључујући анонимне, у погледу питања усклађености, без страха од последица;
- правовремени и конзистентни одговор на „лоше“ понашање, уз одговарајуће дисциплинске мере;
- реализација обуке (са пажњом на улоге, ризике и вредности јасно произашлњ из обуке).

На овај начин се жели истаћи промовисање интегритета етичности, као инструмента узбуњивања (енгл: *whistleblowing*), као снажног подстицаја за превенцију криминалног, односно преватног понашања било запослених у ентитету вило трећих лица. [315]

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

Закон о банкама одређује да у банци постоји организациона јединица у чијем је делокругу рада унутрашња ревизија (Закон о банкама, 2015, члан 85, став 1).

Основни задаци унутрашње ревизије су (Закон о банкама, 2015, члан 85, став 2):

- управном одбору пружа независно и објективно мишљење о питањима која су предмет ревизије;
- обавља саветодавну активност усмерену на унапређење постојећег система унутршњих контрола и пословања банке;

[315] *ibid*

– управном одбору банке пружа помоћ у остваривању њихових циљева, примењујући систематичан, дисциплинован и документован приступ вредновању и унапређењу постојећег начина управљања ризицима, контроле и руковођења процесима.

Банка је дужна да функцију унутрашње ревизије вршпи у складу с прописима који уређују основне принципе организације и рада унутрашње ревизије банке.

Руководилац овог организационог дела има право да се непосредно обрати управном одбору банке када год је потребно, а има и право да предложи сазивање седнице одбора праћење пословања банке, о чему обавештава управни одбор, а ако седница тог одбора не буде одржана, овавештава о томе скупштину банке на првој наредној седници (Закон о банкама, 2015, члан 85, ставови 7 и 8).

Унутрашња ревизија не може обављати друге послове из делатности банке, осим послова који се односе на вршење унутрашње ревизије, нити може учествовати у припреми и изради аката и друге документације који могу бити предмет унутрашње ревизије.

Обавезе унутрашње ревизије су да (Закон о банкама, 2015, члан 85, став 11):

– оцењује адекватност и поузданост система унутрашњих контрола банке и функције контроле усклађености пословања банке;
– обезбеди да се ризици на одговарајући начин идентификују и контролишу;
– утврђује слабости у пословању банке и њених запослених, као и случајеве неизвршења обавеза и прекорачења овлашћења и припрема предлоге за отлањање тих слабости, као и препоруке за њихово спречавање;
– одржава састанке са управним одбором банке, као и одбором за праћење пословања банке;
– редовно припрема извештаје о активностима унутрашње ревизије и доставља их управном одбору банке, као и одбору за праћење пословања банке.

НБС може прописати ближе услове и начин вршења функција унутрашње ревизије.

Запослени у овој пословној функцији имају право увида у све документе банке и њених подређених друштава, као и чланова исте банкарске групе, без ограничења врше надзор над пословањем банке и учествују на седницама управног одбора банке и његових одбора (Закон о банкама, 2015, члан 86).

На захтев унутрашње ревизије запослени су дужни да доставе писано објашњење у вези са слабостима и грешкама у свом раду, као и да их отклоне.

Банка је дужна да НБС достави годишњи извештај о адекватности управљања ризицима и унутрашњој контроли банке (доставља се, у складу са Законом, заједно са годишњим финансијским извештајем). Извештај одобрава управни одбор. Садржину овог извештаја прописује НБС, с тим да он обавезно мора да садржи (Закон о банкама, 2015, члан 87):

– да ли су управни и извршни одбор банке идентификовали значајне ризике;

- да ли су политике унутрашње контроле и управљања ризицима у банци адекватне и да ли се ефикасно примењују;
- да ли су НБС достављени тачни прикази политика управљања ризицима и система унутрашњих контрола;
- да је утврђен план активности за отклањање недостатака и да се примењује или да ће бити утрвђен и достављен на усвајање управном одбору банке.

Љубисављевић је урадила истраживање где је на бази иностране литературе и домаће праксе у остваривању функције унутрашње ревизије, установила колики је ниво развоја интерне ревизије у банкама у Републици Србији, а генерални налаз је да је интерна ревизија у банкама равијенија него у другим привредним субјектима, али је још увек иза међународне праксе у остваривању ових послова.[316]

Емпиријско истраживање је обухватило 14 банака (у време истраживања их је на нашем тржишту било 32), са сврхом да се утврде начини организовања и задаци интерне ревизије у њима. Предмет истраживања је био да се утврди како менаџери и запослени на вишим функцијама у банци разумеју улогу и значај интерне ревизије. Реултати су наведени према следећем:

- величина банке не утиче на организацију и задатке интерне ревизије; интерна ревизија у банкама у РС још увек има нејасан контекст. Светска искуства нису боља, и говоре да 73% услуга интерне ревизије постоји мање од 20 година, па се тако објашњава због чега велики број банака не разуме потпуно ову функцију;
- у РС доминирају стране банке (тада, 64%). Анкетирано је највише централа (54%), филијала (39%) и експозитура (7%);
- Интерна ревизија је организована као сектор (43%), служба (21%) и као одељење (36%), што није увек у корелацији са величином банке;
- Интерна ревизија је подређане управном одбору банке (сматра 29%);
- основни задатак интерних ревизија је оцена усклађености пословања са Законом, политикама, пословном праксом и поступцима менаџмента. Простор за унапређење је: истраживање планова, програма, политика и поступака како би се могло објективно сагледати њихово извршење на свим нивоима. Треба да се укључи и и критичко праћење остваривања укупног плана и појединачних планова, информисање менаџмента и одступање од стандарда и планираних циљева, давање препорука и савета у вези са могућим корекцијама како би се уочена одступања отклонила. Интерна ревизија треба да се више укључи на антиципирање могућих ризика у појединим подручјима пословања банке. Предмет испиривања интерног резизора треба да буде целокупно пословање окренуто будућности;
- Интерна ревизија је организована као самостална организацона јединица, и то обично као сектор. Она је подређена управном одбору и менаџменту банке. У свету

[316] Љубисаввљевић, С.: *Организовање и задаци интерне ревизије у домаћим и страним банкама у Републици Србији*, часопис Економски хоризонти, Јануар-април 2013. године, Економски факултет, Универзитет у Крагујевцу, 2013. година

влада мишљење да је најбоље када је интерна ревизија подређена највишем руководству, а код нас је то само делимично испуњено. Поред подређености управном одбору, код нас постоји и подређеност менаџменту банке. Код мањег броја испитаника постоји подређеност извршном одбору и одбору за ревизију. Подређеност скупштини акционара, као највишем руководству, код нас постоји у врло малом броју случајева;

- у РС је потребно радити на едукацији организација, јер су неки послови интерних ревизија запостављени. Код нас је приоритет откривање и спречавање грешака и нелегалних радњи, као и оцена усклађености пословања са законом, политикама и пословном праксом банке. Остали задаци које треба развијати су: оцена успешности рачуноводственог система и систем унутрашњих контрола и благовремено састављање квалитетних финансијских извештаја и додавање вредоности акцијама.У свету су ови задаци врло развијени;
- тренд у додавању послова интерне ревизије је: ревизија квалитета, ревизија животне околине, развој предузетништва, менаџмента, стратегија и сл.;
- Интерна ревизија је интерни саветник који нема репресивни већ заштитни карактер. Она је функција која контролише све остале функције у банци.

Приказано истраживање је привукло нашу пажњу због условне сличности пословних функција усклађености пословања, интерне ревизије и безбедности. Све функције са на неки начин баве ризицима, а специфичност безбедности је да се тежишно бави оперативним ризицима, одакле сматрамо да би будућа истраживања у области безбедности могла да користе сличну платформу као наведено истраживање.

Такође мишљења смо да би истраживања у овим областима, слично као што је представила Љубисављевић, дала научно верфиковане чињенице о правцима у којима треба да се крећу банке, како би унапредили ове фукционалности.

Станишић наводи да је интерна ревизија независна функција о оквиру банке, чији је задатак да испита ризике са којима се банка суочава (дакле све ризике, наша је примедба), да провери адекватност интерних контрола које се обављају ради заштите тих ризика (дакле и ризика који угрожавају информациону безбедност, наша је примедба), и – да верификује да контроле функционишу како је планирано. *Ризик у организацији је полазна тачка ревизора*. Директор интерне ревизије треба да обезбеди да интерни ревизори поседују потребно *искуство, образовање, обуку и стручност* за правилно оцењивање интерних контрола и процењивање ризика.[317]

На нивоу опажања у практичном остваривању послова безбедности, интерне ревизије и усклађености пословања у банкама, ми смо приметили да би спровођење истраживања, како смо већ навели, дало извесно одступање од неких начела које је навео Станишић, а пре свега у погледу компетенција кадрова који обављају ове послове. Индикативан је и податак из истраживања Љубисављевић, где је нашла да (само) 29% испитаника у њеном истраживању

[317] Станишић, М.: *Карактеристике модерне ревизије у банкама*, Банкарство 7-8, 2007. године, доступно на: https://www.ubs-asb.com/Portals/0/Casopis/2007/7_8/UBS-Bankarstvo-7-8-2007-Stanisic.pdf

сматра да је Интерна ревизија подређена управном одбору банке, а видели смо у Закону у којој мери је овај организациони део везан управно за управне одборе банака.

3.7. Организација банке по пословима

Видели смо из досадашњег истраживања да су банке комплексне организације, у којима се обавља већи број различитих пословних функција, као и да неке од тих функције, као што су *Compliance, Internal Audit* і *Security* имају одређене додирне тачке, или – у најмању руку имају исте сличну природу у погледе заштиту организације од различитих врста ризика. Ову особину коментарисали смо и у оквиру поглавља где смо разматрали могуће моделе организовања послова заштите информација у организацијама.

Остале пословне функције у банкама, такође имају свој допринос у остваривању циљева организације, а у банкама су организоване на сличним принципима, са свим својим специфичностима сваке банке понаособ.

Хаџић сматра да организација банке подразумева њену унутрашњу организациону шему, организацију рада и начин управљања.[318]

Организација банке се утврђује статутом банке, а како у Закону нема прецизних одредби, ова активност је препуштена самим банкама, у оквиру начела која је Закон дао.

Фактори који утичу на то какву ће организацију банка имати (од чега то зависи), дати су према следећем:[319]

- величина банке, као и обим послова;
- врсте послова које банка обавља;
- развијеност пословне мреже банке;
- степен рационализације;
- врста клијената банке (привреда, становништво, друго);
- банкарски обичаји;
- степен организованости финансијског тржишта.

Свим банкама је заједничка карактеристика одвајање управљачког од извршног дела организације, као и да се извршни апарат дели на секторе, сектори на дирекције, а дирекција на одељења.[320]

Да оваква организациона подела није обавезујућа, упућује нас искуствено опажање, где смо приметили да неке банке могу другачије да називају своје организационе целине, али је

[318] Хаџић, М., *op.cit.*, стр. 127.-131.

[319] *Ibid*
[320] *Ibid*

принцип субоординације и координације увек присутан (на пример: сектор, одељење, одсек).

Руководећи се организационим моделом како је дао Хаџић, даћемо и следеће ближе одређење:

- *Сектор*, представља организациону јединицу која се формира по најважнијим групама послова (пословним линијама, или пословним функцијама). У зависности од значаја који се придаје појединим групама послова, зависи и да ли ће поједини послови вити организовани у вишу или нижу организациону форму. Такође, наша је примедба да одређивање организационог нивоа послова може да зависи и од броја ангажованих извршилаца, величине буџета, циљева организације и слично. Неки од најчешћих сектора у банкама су:

  - рад са становништвом (енгл: *Retail*);
  - послови са привредом (енгл: *Corporate*);
  - послови са иностранством;
  - Послови средстава ликвидности – Трезор.

  На челу сектора налазе се директор или извршни директори, који се непосредно потчињавају председнику ИО (извршни одбор – ИО), а заједно са њим формирају менаџмент тим банке. Управни одбор своја овлашћења преноси на ИО, у смислу свакодневног функционисања и вођења „дневне“ политике банке, а за реализацију су задужени поједини сектори.

- *Дирекција* је организацона јединица у оквиру сектора, а у њима се обављају важније групе послова, као што су:

  - Дирекција за кредите;
  - Дирекција за девизно-валутне послове;
  - Дирекција за кредите са иностранством;
  - Дирекција за платне картице;
  - Дирекција за *e-banking.*

- *Одељења* су организационе јединице које се формирају по ужој специјалности у оквиру једне дирекције, односно сектора непосредно. Структура одељења зависи од њихових размера. Ако обухвата више сродник послова (на пример, у Одељењу безбедности: физичко-техничка заштита, безбедност и здравље на раду, заштита информација, заштита од пожара, интерне истраге и друго), дели се на одсеке, а ови на групе (на претходно наведеном примеру: у оквиру одсека физичко-техничке заштите, група за техничку заштиту, група за физичку заштиту и сл.). Банкарска одељења по својим функцијама могу да се поделе на три групе: централна (раде послове за целу банку, обухватајући и територијалну организацију и у том смислу представљају везу периферних организационихи целина и дирекције, као што су:

HR, Security, Одељење за организацију, Одељење за правне послове и друго), пословна одељења обављају банкарске послове и карактеристика им је што долазе у контакт са клијентима банке (као што су: благајна, девизно-валутно, хипотекарно и друго), административна одељења својим радом омогућавају уредно функционисање администрације (као што је: економат, архива, експедиција поште и друго).

Поједине банке могу бити организоване као холдинг предузећа, када настоје да финансијски прате групу повезаних предузећа (корпоративне банке). У њиховој организацији се јављају супсидијарна предузећа, повезана са банком (обично у трговини, туризму и производњи). Такође, холдинг могу да направе и банке које су развиле и друге врсте послова који се односе на финансије, као што су компаније које се баве осигурањем, консалтингом, брокерско-дилерске компаније и лизинг компаније.

3.8. Територијална организованост банака

У зависности од својих пословних циљева, банке теже ка стварању што боље мреже за продају услуга/производа, посебно уколико им се пословна стратегија заснива на послу са становништвом.

На једној страни постоји потреба за специјализацијом појединих пословних јединa за одређене врсте делатности, а на другој је тенденција за што непосреднијим контактом са клијентима.

Доба нове технолошке револиције донекле мења ову слику, будући да су клијенти све спремнији да користе дигиталне сервисе и услуге, а банке се већ припремају за такав масовни вид пословања, и то, наше је мишљење из најмање два разлога. Један је да је вишегодишњи тренд у банкам да се смањи број особља у циљу уштеда, као и да се смање трошкови које банке одвајају за своје пословне просторе, а други, посебно важан са аспекта заштите информација у банкама, да све више услуга и сервиса, уз технолошке напретке, у банкама желе да обављају сами клијенти (може и да се каже да банке желе да клијенти буду што ефикасније услужени, или да банке желе да смање број запослених, односно све то заједно), одакле ће банка будућности вероватно бити само пословни простор који деле клијенти и „машине“, а велики број сервиса клијенти ће обављати и без доласка у пословни простор банке – на даљину. Ове пословне промене ће сасвим извесно убрзо довести и до промене физиономије безбедности у банкама и финансијским институцијама, будући да ће се променити и извори и облици угрожавања пословања.

Ипак, традиционално банкарство још увек се заснива на мрежи екпозитура, које су, осим уважавања географске покривености територије, организоване и према припадајућем нивоу пословне категорије.

Хаџић сматра да у смислу претходно наведеног банке познају следеће пословне јединице:[321]

Главна централа, у хијерархијском смислу на навишем месту у организационој шеми банке и у њој се налази управа банке. Ту се обављају следећи послови: утврђује се пословна политика, дају упутства за реализацију пословне политике, координира и контролише рад централе и осталих пословних јединица нижих нивоа. Делатност јој се простире на цело подручје одређене земље. Главна централа доноси и одобрава план и завршни рачун банке.

Централа, представља пословну јединицу која је по рангу одмах иза главне централе. Обим њене самосталности и однос према централи је различит, зависно од организационе структуре банке. Овде је најчешће реч о већој територији на подручју одређене земље. Централа координира и контролише рад главних филијала и осталих пословних јединица.

Главна филијала је пословна јединица која је по својим карактеристикама слична централи, с том разликом што је њено пословно подручје на којем делује уже, а степен самосталности у раду мањи.

Филијала, је основни облик пословне јединице. Помоћу мреже филијала банка остварује јединсто кредитног и платног промета, као и јединство средстава, а сврха оснивања филијала је ширење послова на што веће подручје.

Афилијација представља посебну организациону целину банке у иностранству, када банка намерава да прошири подручја деловања на другу земљу.

Експозитура је пословна јединица банке која се оснива у местима за која је банка проценила да имају пословни потенцијал за обављање њене делатности. Ово је заправо истурени пункт банке и ту се обављају шалтерски послови. Њихово књиговодство се ослања на више пословне јединице.

Платна испостава је пословна јединица банке која служи само за уплату и исплату у одређеном већем месту, док све друге налоге шаље на извршење у филијалу. Платна испостава ради само повремено и у одређене дане и то са особљем филијале.

Депозитна каса је пословна јединица банке која је по делатности врло слична платној испостави, с тим што ради стално и има своје особље.

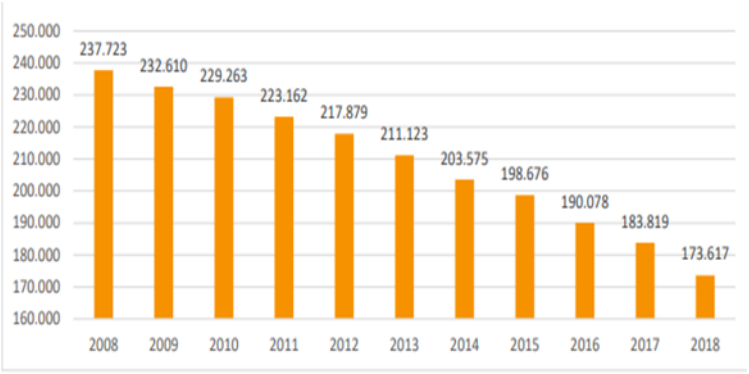
Чињеница је да велике банке имају и развијене мреже филијала, као и да је и у свету у банкарском сектору присутан тренд смањења њихових мрежа[322], што је, наше је мишљење, иницирано наступањем претходне светске економске кризе, а подржано дигитализацијом и променом профила банкарских услуга (Графикон број 10: *Број пословница (бренчева) у ЕУ у периоду од 2008. – 2018. године*).

.

[321] *Ibid*, стр. 131. – 132.

[322] Графикон броја бренчева у ЕУ у периоду 2008. - 2018. година, *Banking in Europe: EBF Facts & Figures 2019*, European Banking Federation, 2019., стр. 12., доступно на: https://www.ebf.eu/wp-content/uploads/2020/01/EBF-Facts-and-Figures-2019-Banking-in-Europe.pdf

Графикон број 10: ***Број пословница (бренчева) у ЕУ у периоду од 2008. – 2018. године***



Б. Грегановић, у тексту о дигиталној трансформацији банака каже: ..“дигитализација је промена која тражи од банака нов начин размишљања, нов приступ клијентима, продаји, маркетингу и свим другим активностима, ... , мера у којој ми банкари, препознамо то окружење и научимо да одговоримо на његове изазове пресудна је за наш положај, па и опстанак на тржишту, ... , дигитализација тражи кореницу промену у начину размишљања у организацији“... [323]

3.9. Банкарски ризици

Ризик је један од појмова, слично као и безбедност, који су често у употреби у свакодневном животу савремене људске заједнице, одакле се он спомиње не само у науци већ и у привреди и у свакодневном животу.

Одређењем ризика бави се и стандард ISO 31000, који даје смернице како компаније могу да донесе одлуке у управљању, планирању, извешавању, одређивању политика, својих вредности и култура.[324]

У банкарству, област ризика је једна од основних пословних функција и у том смислу преставља пословну функцију која је саставни део нормативног оквира пословања на међународном и државном нивоу.

Хаџић наводи да је у савременим условима, поготово у условима глобалног пословања банкарства присутно много ризика који доводе у питање појединачне банкарске послове,

[323] Грегановић, Б.: *Дигитална трансформација банака није само креирање апликације – то је промена начина размишљања*, председник Извршног одбора НЛБ банке, Београд, 2019. година, доступно на: https://www.netokracija.rs/digitalna-transformacija-banke-161180

[324] Доступно на: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf

наплату или у крајњем случају промену, која утиче на повећање неизвесности исхода трансакције и у целини повећава неизвесност остваривања прихода банке.[325]

Светска економска криза из 2008. године потврђује да је развојем инвестиционог банкарства и процесом глобализаије финансијског система дошло до додатног увећања ризика са којим се банке суочавају.[326]

Ризик представља могућност да ће се неповољан стицај околности десити. Ризик може бити материјалан и нематеријалан. *Материјани ризик* је могућност губитка на трансакцији, клијенту или послу. *Нематеријални ризик* представља могућност, да може доћи до нарушавања угледа банке. Углед је степен поверења у појединачном банкарству, чије нарушавање може угрозити њено пословање. Ризик пословања банке се, озбиром на природу банке као новчане организације, исказује у новчаном износу, без обзира о којој врсти ризика је реч. Он се не може у потпуности елиминисати, већ се само може свести на разумну меру.[327]

У литератури постоје различите дефиниције ризика, а најважније су, како наводи Хаџић, следеће:[328]

- вероватноћа губитка или изложености губитку;
- могућност или шансе за настанак губитка;
- опасност која може проузроковати губитак;
- опасни подухват или услови који повећавају вероватноћу учесталости или озбиљности од губитка;
- имовина или особа изложена губитку;
- губитак потенцијалног износа новца;
- одступање од стварних губитака;
- могућност да стварни губици одступају од очекиваних;
- неизвесност у односу на губитак.

Фактори ризика пословања банака могу се свести на *TRICK* формулу (енгл: *Technology risk, Regulatory risk, Interest rate risk, Client risk, Capital adequacy risk*), према следећем:

- *T* – ризик технологије се јавља због проблема везаних за технологију, а укључује негативне последцие на зараду банака, профит и капитал. У вези руковођења савремених IT система, са развојем информатике дошло је до масовне употребе електронике у банкама у хардверском и софтверском смислу, од обраде информација до обраде обраде захтева клијента и њихових рачуна;
- *R* – ризик промене регулативе је ризик који настаје са изменом закона и других прописа;

[325] [325] Хаџић, М., *op.cit*., стр. 294.- 309.
[326] *Ibid*
[327] *Ibid*

[328] *Ibid*

- *I* – је ризик каматне стопе који настаје услед промена каматних стопа;
- *C* – ризик корисника се односи на могућност да клијент банке буде преузет од конкурентских банака;
- *K* – ризик адекватности капитала, или ризик солвентности настаје ако се испуне претходно наведени ризици, чиме банка улази у зону неусклађености са међународним стандардима банкарског пословања, који су укључени у национално законодавство, чиме се доводи у питање и одобрење за пословање од стране регулатора.

Банка идентификује, мери и процењује ризике којима је изложена у свом пословању и управља тим ризицима и *дужна је да образује посебну организациону јединицу у чијем делокругу рада је управљање ризицима*, наводе Џелетовић и сарадници.[329]

Банка прописује процедуре за идентификовање, мерење и процену ризика, као и управљање ризицима, својим актима који садрже:[330]

- одредбе којима се обезбеђује функционална и организациона одвојеност активности управљања ризицима и редовних пословних активности банке;
- процедуре за идентификовање, мерење и процене ризика;
- процедуре за управљање ризицима;
- процедуре којима се обезбеђује контрола и доследна примена свих унутрашњих процедура банке у вези са управљањем ризицима;
- процедуре за редовно извешавање органа банке и регулаторног тела о управљању ризицима.

Банка у свом пословању препознаје више врста ризика, од којих издвајамо:

Ризик ликвидности, је ризик могућности настанка негативних ефеката на финансијски резултат и капитал банке услед неспособности те банке да испуњава своје доспеле обавезе. Ради ефикасног управљања овом врстом ризика *надлежни орган банке усваја и спроводи политику управљања ликвидношћу*, која обухвата планирање прилива и одлива новчаних средстава, праћење ликвидности и доношење одговарајућих мера за спречавање или отклањање узрока неликвидности. *НБС прописује начин утврђивања и нивое ликвидности банке*, укључујући и критично низак ниво ликвидности.[331]

Кредитни ризик, је ризик настанка негативних ефеката на финансијски резлултат и капитал банке улсед неизвршавања обавеза дужника према банци. Банка је дужна да кредитни ризик идентификује, мери и процењује према кредитној способности дужника и његовој уредности у извршавању обавеза према банци, као и према квалитету инструмената обезбеђења потраживања банке. У складу са прописима НБС, банка је дужна обрачунава и

[329] Џелетовић, М., Живковић, А., Бојовић, П., *op.cit*, стр. 138. – 141.
[330] *Ibid*

[331] *Ibid*

издваја резерве за процењене губитке који могу настати по основу биласне активе и ванбаласних ставки банке. Банка је дужна да својим унутрашњим актима пропише посебне политике и процедуре за идентификовање лоше активе и управљање том активом, као и за редовно извештавање органа банке о квалитету кредитног портфолија.[332]

Каматни ризик је ризик могућности настанка негетивних ефеката на финансијски резултат и капитал банке услед промена каматних стопа.

Девизни ризик је ризик могућности настанка негативних ефеката на финансијски резултат и капитал банке услед промене девизног курса. Својим унутрашњим актима банка је дужна да пропише посебне политике и процедуре за идентификовање тржишних ризика у управљање овим ризицима, као и за редовно извештавање органа банке о врстама и нивоу ризика.[333]

Оперативни ризик је ризик могућности настанка негативних ефеката на финансијски резултат и капитал банке *услед пропуста у раду запослених, неодговарајућих унутрашњих процедура и процеса, неадекватног управљања информационим и другим системима, као и услед непредвидивих екстерних догађаја*.[334]

НБС прописује критеријуме за идентификовање, мерење и процену ризика, као и за управљање ризицима, укључујући и: начин израчунавања појединачних показатеља пословања банке у вези са управљањем ризицима и ограничења која се односе на те ризике; начин, форму и рокове извештавања банке о показатељима.

Јасно је да по свом одређењу, *оперативни ризици привлаче нашу највећу пажњу*, будући да се непосредно односе на предмет нашег истраживања – заштиту информација у функцији безбедности пословања банака и финансијских институција. Како смо видели, они обухватају и *пропусте у раду запослених* (на које у великој мери утичу организацоне мере, безбедносна култура организације, као и нормативне мере, кроз одређење оперативних ризика да настају услед *неодоварајућих унутрашњих процедура и процеса*, и друго), али и *неадекватног управаљања информацијама и другим системима*, а посебно – *услед непредвиђених екстерних догађаја*.

Тако смо у блиској историји могли да видимо колико утицаја на пословање банака имају елементарне непогоде (поплаве у Ребулици Србији 2014. године), али и појава епидемија и криза изазазвана пандемијским вирусом Корона. Банке су у том смислу морале да донесу више мера и активности, почевши од промене организације рада (промене у радном времену, промене у правилима боравка запослених и клијената у просторијама банака, увођење мораторијума на отплату кредита од стране НБС, прелазак на масовни рад од куће и друго.). Рад од куће је сасвим извесно, због своје масовности и због своје дискутабилне

[332] *Ibid*

[333] *Ibid*

[334] *Ibid*

припремљености банака на овакав облик пословања, што ће тек бити, наше је мишљење, предмет истраживања научних и стручних радова у свету и од нас, створио нову врсту ризика, а посебно са аспекта угрожености пословања банака у сфери заштите информација.

Полазећи од репрезентативности ове кризе и њеног значаја за наш предмет истраживања, одлучили смо се да посебан простор у нашем истраживању, а као мали допринос будућим радовима, посветимо утицају ове кризе на банкарско пословање.

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

Криза изазвана корона вирусом је, између осталог, типичан пример како један ризик, и ако по својој фенеменологији долази из сфере оперативних ризика, може да се због свог појавног облика прелије и на друге сфере ризика (као што су ризик ликвидности и кредитни ризик), што ће, такође смо уверени, тек имати своје импликације кроз нову кризу која ће уследити на светску економију изазване овом појавом.

Европска банкарса агенција (енгл: *European Banking Authority – EBA*)[335], сматра да је корона вирус створио значајне изазове друштву и ризике за економску прогнозу. Дугорочне последице још увек нису сагледиве, али готово сигурно се може предвидети смањење економске активности. Финансијска криза је допринела да европске банке побољшају квалитет активе у својим билансима, као и да спроведу мере континуитета пословања и да се усредсреде на оперативне ризике, одакле су се опет концентрисале на своје основне операције и критичне функције.

Оперативни изазови са којима банке могу да се суоче треба да буду приоритет, сматра ЕБА, а с тим у вези су одлучила да одложи планирани *стрес тест* на нивоу ЕУ за 2021. годину, како би били у прилици да банкама доставе ажуриране информације о изложености банака.

Пандемија *COVID 19,* је глобални стресни догађај који тестира финансијску, оперативну и комерцијалну отпорност организација. У том контексту сектор финансијских услуга мора да се брзо и обимно припреми и прилагоди тренутним ограничењима и тржишним условима.

До данас, компаније су за приоритете имале финансијске и оперативне мере, као пто су заштита ликвидности и новчаних токова, као и предузимање мера које гарантују наставак пословних активности. Регулатори су предузели кораке ка ублажавању притисака, као што је већ одлагање наведеног стрес теста, и померање контролних прегледа, тамо где је то

[335] Европска банкарска агецнија је независно тело ЕУ са улогом регулације и дазора у банкарском сектору у Европи. Њени општи циљеви су одржавање банкарске стабилности у ЕУ и очување интегритета, ефикасности и уредног функционисања банкарског сектора. Главни задатак је да допринесе стварању јединствених правила у банкарству на овом простору. Ауторитет се засвнима на овлашћености да врши процену ризика и рањивости у банкарском сектору ЕУ. Основана је 1. јануара 2011. године као део ефропског система финансијског надзора и преузела је све одговорности и задатке Комитета европских банкарских супервизора. Доступно на: https://eba.europa.eu/about-us/eba-at-a-glance

могуће, наводи се у тексту *KPMG*-а о потреби хитног реаговања финансијског сектора на последице корона кризе.[336]

Очекивања су да ће се у наредном периоду (а то значи да се ове претње догађају масовно у тренуцима писања овог рада), видети како је банкарски сектор реаговао на настајуће претње, као што су преваре (енгл: fraud), безбедност података (енгл: data security) и спречавање прања новца (енгл: Anti Money Laundering – AML) и *Costumer Due Diligence*[337].

Преваре; Индустрија финансијских услуга изложена је ризику од повећаног нивоа превара, *укључујући cyber преваре*. У Британији, Национална агенција за криминал (енгл: *National Crime Agency – NCA*)[338] је објавила да појачано ажурира податке о преварама које су у вези са *COVID 19*, а да ће сигурно доћи до повећања превара „овлашћених плаћања", које уствари представљају преваре са банковним трансферима. Преваре се односе на полисе осигурања, пензијске фондове, инвестиције са неоубичајено великим обртом, укључујући улагања у крипто валуте. Извршиоци су изузетно софистицирани, стручни, упорни и добро знају да процене рањиве мете.

Сајбер резилијентност (енгл: *Cyber resilience*); сајбер напади су се дефинитвно повећали, у распону од крађе идентитета до софистицираних напада на мреже и проток информација. Организације ће морати више него икада да појачају своју сајбер одбрану и едукују запослене на свим нивоима за нове ризике.

Безбедност података; даљински рад (или рад од куће) постаје норма, одакле је потребно размотрити на који начин се приступа подацима и како се они штите. Запослени раде са безбедносно осетљивим подацима у сасвим сигурно мање сигурним окружењима, као што су кућна окружења, одакле се под хитно мора направити равнотежа између овог амбијента и безбедности која је „закључана" иза корпоративног заштитног зида. Овај зид мора постати лакше доступан запосленима и пословним партнерима, како би се са једне стране наставили пословни процеси и операције, а са друге стране, он мора нападачима и даље да отежава приступ осетљивим информацијама. Прописи попут GDPR-а се и даље примењују, одакле

---

[336] *COVID-19 Insights – Emerging Risks, Financial services sector is having to adapt rapidly, KPMG, 2020*. Доступно на: https://home.kpmg/xx/en/home/insights/2020/04/covid-19-insights-emerging-risks.html

[337] *Due Diligence* је у најкраћем: процес анализирања пословног субјекта пре, за време и

после пословне трансакције. Да би пружио комплетну слику мора да садржи финансијску, пореску, правну анализу, анлизе технологија, људских ресура и пословних операција. Доступно на: https://marketnetwork.rs/?p=25068

[338] *National Crime Agency (NCA*), бави се сузбијањем најтежих дела тешког и организованог криминала у Великој Британији, доступно на: https://www.nationalcrimeagency.gov.uk/who-we-are/our-mission

ће руководиоци за ризик и поштовање правила морати да изврше преиспитивање повезаних ризика и да примене алтернативне мере које ће довести до ублажавања.[339]

Спречавање прања новца и финансирање тероризма и Costumer Due Diligence; показује слабост услед мера социјалног дистанцирања, што доводи до објективног смањивања тимова који се баве овим проблемима и вероватно до прескакања неких корака у проверама које се уобичајено одвијају. Очекује се да процеси контроле, услед наведеног, сада буду неповезани и мање квалитетни због рада од куће. Са друге стране, захтеви за оваквим проверавама су знатно увећани (због повећаних ризика у свим сферама), и очекује се брзо поступање и решавање захтева – дакле пуно захтева за оваквим проверама који морају да се реше „сада и одмах“, уз могуће одустајање од квалитета провера.

Промене у сфери понашања запослених; сасвим сигурно наступају са *COVID-ом,* јер некоме се допада већа самосталност, а некоме не одговара, што организације доводи у ситуацију да морају да решавају питања „менталног благостања“ и повезаности запослених. Менаџери у оваквим околностима имају отежане околности јер ће сигурно доћи до пада ефикасности, барем краткорочно. У том смислу морају се успоставити нови ланци управљања. Организације које су боље припремљене за рад од куће запослених, у организационом смислу, вероватно ће се боље прилагодити, док ће оне где је владао аутократски модел управљања менаџера бити пре великим искушењем. Такође, сви су у овим околностима изложени новим финансијским притисцима, и појединци и организације, што ће довести до некарактеристичног понашања, а у најекстремнијим случајевима, и до појачаног ризика од интерних превара.

Посебан проблем ће донети понашање регулатора, јер ће новонастале околности довести до „разумевања“ околности, па ће доћи и до извесног опуштања у смислу охрабривања привредних субјеката да сарађују и поред погоршаних околности (безбедности).

Дужина трајања *COVID* кризе још никоме није позната, а посебно не импликације које ће се јавити на пословање. Из ових разлога ће организације морати да се посвете дугорочном прилагођавању радне праксе и новој организационој култури (у нашем раду управо говоримо о овим променама као дуготрајном процесу у којем организације морају да покажу истрајност и континуитет активности).

Регулатори ће несумњиво давати нове смернице (у области банкарства сасвим извесно), али и поред тога ће организације морати да буду проактивне у решавању новонасталих ризика (дакле не по својој феноменологији нових, али нових по актуелности и обиму наступања) и посебно у промени приоритета које одређују у циљу постизања пословних циљева.

[339] GDPR – *General Data Protection Regulation*, регулише приватност и заштиту података о личности осова на територији ЕУ. Ова регулатива омогућава строжу контролу корпорација како не би дошло до злоупотребе личних података корисника. Прецизније се дефинише начин на који неко може да прикупља, складишти и продаје личне податке. Прецизније је дефинисано шта се сматра под личним податком, па се тако и IP адреса изједначава са другим информацијама о кориснику. Доступно на: https://www.it-akademija.com/sta-je-gdpr

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

У досадашњем објашњењу нормативне регулисаности заштите информација у Републици Србији истакли смо да нормативни оквир заштите информација у банкама и финансијским институцијама треба посматрати у међународном, државном и локалном контексту, односно на нивоу самих друштава.

У том смислу, дали смо преглед уставног и законског оквира заштите података, законске регулативе прикупљања и обраде и заштите података, појам тајности података и заштите пословне тајне, сагледали смо заштиту података о личности и слободан приступ информацијама о јавног значаја, прописе који се односе на информациону безбедност и одредили смо појам интерних аката правног лица у овој области, кроз улоге правилника о пословној тајни, правилника о приватности и интерних безбедносних правила и процедура.

Нормативно уређење области заштите информација у банкама и финансијским установама ближе је регулисано актима које доноси Народна банка Србије, одакле ћемо у даљем тексту приказати Закон о банкама, Одлуку о мининалним стандардима управљања информационим системом финансијске институције и Одлуку о управљању ризицима банке.

4.1. Закон о банкама

Закон о банкама уређује оснивање, пословање и организацију бананка, начин управљања банкама, као и контролу, реструктуирање и престанак рада банака (Закон о банкама, 2015, члан 1).

Полазећи од предмета истраживања нашег рада, нама је од значаја да се упознамо како законодавац дефинише материју која се посредно или непосредно односи на уређење заштите информација у њима, односно како се у Закону третира управљање ризицима.

Банка је одређена како акционарско друштво, са седиштем у Републици Србији, које има дозволу за рад Народне банке Србије и обавља депозитне и кредитне послове. Одеђено је да она може обављати и друге послове у складу са законом (Закон о банкама, 2015, члан 2, став 1).

Страна банка је правно лице са седиштем ван Републике Србије које је, у складу са прописима државе порекла, основано и у регистар надлежинх органана те државе уписано као банка, које поседује дозволу за рад регулаторног тела те државе и које обавља депозитне и кредитне послове (Закон о банкама, 2015, члан 2, став 2).

Из претходних одређења видимо да се домаће и стране банке идентично одређују, те да морају да обављају депозитне и кредитне послове, односно друге послове у складу са законом, за шта морају да имају одобрење надлежног регулатора државе у којој су основане.

Регулаторно тело је национално тело које прописима одређене државе овлашћено да даје и одузима дозволе за рад лицима у финансијском сектору, врши контролу ових лица, односно надзор над тим лицима или уређује њихово пословање, као и одговарајуће тело Европске уније са овим надлежностима у складу с прописима те уније (Закон о банкама, 2015, члан 2, став 5).

Филијала је организациони део банке, без статуса правног лица, који обавља послове које може обављати банка у складу са законом (Закон о банкама, 2015, члан 2, став 3).

Банкарска група је група друштава коју чине искључиво лица у финансијском сектору и у којој најмање једна банка има својство највишег матичног друштва или својство зависног друштва (Закон о банкама, 2015, члан 2, став 21). Банакарски холдинг је највише матично друштво у банкарској групи које није банка. Ако се матично друштво не може поуздано утврдити, њега утврђује Народна банка Србије ((Закон о банкама, 2015, члан 2, став 22).

Критичне пословне функције су активности, услуге или послови чији би прекид обављања вероватно довео до угрожавања ставилности финансијског система или поремећаја у пружању неопходних услуга реалном сектору услед величине, тржишног учешћа и повезаности субјекта који их обавља са осталим учесницима у финансијском систему, а нарочито узимајући у обзир могућност да неко други несметано преузме обављање тих активности, услуга или послова (Закон о банкама, 2015, члан 2, став 29).

Послови које банка може обављати одређени су према следећем (Закон о банкама, 2015, члан 4):

1) депозитне послове (примање и полагање депозита);
2) кредитне послове (давање и узимање кредита);
3) девизне, девизно-валутне и мењачке послове;
4) послове платног промета;
5) издавање платних картица;
6) послове с хартијама од вредности;
7) брокерско-дилерске послове;
8) издавање гаранција, авала и других облика јемства (гаранцијски посао);
9) куповину, продају и наплату потраживања;
10) послове заступања у осигурању;
11) послове за које је овлашћена законом;
12) друге послове чија је природа сродна или повезана с пословима наведеним од тачке 1) до 11), у складу са оснивачким актом и статутом банке.

Послове заступања у осигурању банка може обављати уз претходну сагласност НБС.

Сарадња НБС у вези с контролном функцијом и реструктуирањем, одређена је Чланом 8, где је наведено да НБС сарађује с домаћим и страним регулаторним телима ради вршења у унапређивања своје контролне функције (Закон о банкама, 2015, члан 8, став 1). У ту сврху она може размењивати податке (информације) прибављене у вршењу своје контролне функције, као и других послова утврђених законом, ако је обавеза чувања тајних података једнака обавези утврђених касније у Закону или строжа од ње (Закон о банкама, 2015, члан 8, став 3).

НБС, запослени у НБС, лица која је НБС именовала за привремене управнике или посебне управнике, као и друга лица која по решењу НБС или на основу овог закона у поступку контроле или реструктуирања врше дужности утврђене овим законом, не одговарају за штету која настане вршењем тих дужности, осим ако се докаже да нису поступали по доброј вери (Закон о банкама, 2015, члан 9а, став 1).

Подаци који се односе на контролу бонитета и законитости пословања банке и на реструктуирање банке, као и документи који садрже такве податке, а које запослени у НБС, агенцији надлежној за осигурање депозита, министарству надлежном за послове финансија или банци и друга лица на било који начин сазнају у обављању послова у вези са контролом, односно реструктуирањем, одређују се и штите се као тајни подаци са ознаком степена тајности „СТРОГО ПОВЕРЉИВО“, „ПОВЕРЉИВО“ или „ИНТЕРНО“, у складу са законом који уређује тајност података (Закон о банкама, 2015, члан 9б, став 1).

Истим чланом је одређено да су ова лица дужна да чувају податке и документе као тајне податке, односно не могу их учинити доступним трећим лицима, осим у случајевима прописаним законом. Ова обаеза не престаје ни након престанка радног односа, односно ангажовања, као ни након престанка другог својства на основу ког су ова лица остварила приступ подацима (Закон о банкама, 2015, члан 9б, став 3). НБС може ове податке учинити доступним домаћим и страним регулаторним телима, под условом да их та тела користе искључиво у сврхе за које су прибављени (Закон о банкама, 2015, члан 9б, став 4).

НБС одређује као тајни податак податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета и за који је, у поступку одређивања података као тајних, утврдила да је потреба заштите интереса РС претежнија од интереса за слободан приступ информацијама од јавног значаја (Закон о банкама, 2015, члан 9б, став 5).

Чланом 14 одређено је шта све садржи Статут банке, па је између осталог наведено да садржи начин вршења унутрашње контроле и унутрашње ревизије банке и податке и исправе који се сматрају пословном тајном банке и начин поступања с тим подацима и исправама (Закон о банкама, 2015, члан 14, ставови 7 и 8).

Дозволу за рад банке НБС даје после давања прелиминарног одобрења и подношења захтева за давање дозволе, а уз захтев оснивачи достављају и доказ о томе да су ангажовали спољног ревизора банке и податке о организационој структури и кадровској оспособљености банке (Закон о банкама, 2015, члан 18, тачке 3 и 4).

Управљње ризицима је одређено у Члану 28, где се експлицитно наводи да банка идентификује, мери и процењује ризике којима је изложена у свом пословању и управља тим ризицима (Закон о банкама, 2015, члан 28, став 1).

Банка је дужна да образује посебну организациону јединицу у чијем је делокругу рада управљање ризицима (Закон о банкама, 2015, члан 28, став 2).

Банка је дужна да обезбеди функционалну и организациону одвојеност активности управљања ризицима и редовних пословних активности банке. Управљање ризицима усклађује се с величином и организационом структуром банке, обимом њене активности и врстама послова које банка обавља (Закон о банкама, 2015, члан 28, ставови 3 и 4).

Наведено је и да банка својим актима прописује стратегију и политике за управљање ризицима, стратегију управљања капиталом, процедуре за идентификовање, мерење и процену ризика, као и управљање ризицима, у складу с прописима, стандардима и правилима струке, и то (Закон о банкама, 2015, члан 28, став 5):

1) процедуре за идентификовање, мерење и процену ризика;
2) процедуре за управљање ризицима;
3) процедуре којима се обезбеђује контрола и доследна примена свих унутрашњих аката банке у вези са управљањем ризицима
4) процедуре за редовно извештавање органа управе банке и реглаторног тела о управљању ризицима.

НБС може да пропише ближе услове и начин идентификације, мерења и процене ризика, као и управљање тим ризицима (Закон о банкама, 2015, члан 28, став 7).

Од посебног значаја за предмет истраживања је Члан 29, који наводи врсте ризика, као и да се актима из претходног члана морају обухватити све врсте ризика којима је банка изложена у свом пословању. Посебно су наведене следеће врсте ризика (Закон о банкама, 2015, члан 29, став 1, тачке 1 до 7):

1) ризик ликвидности;
2) кредитни ризик;
3) каматрни и девизни ризик и остали тржишни ризици;
4) ризици изложености баке према једном лицу или групи повезаних лица
5) ризици улагања банке у друга правна лица и у основна средства и инвестиционе некретнине банке;
6) ризици који се односе на земљу порекла лица према коме је банка изложена;
7) оперативни ризик, укључујући правни ризик, као и ризик неодговарајућег управљања информационим и других технологијама значајним за пословање банке.

У каснијим одредбама дефинишу се поједине врсте ризика, а за наше истраживање је од посебно значаја одређивање оперативног ризика.

Оперативни ризик је могућност настанка негативних ефеката на финансијски резултат и капирал банке услед пропуста у раду запослених, неодговарајућих унутрашњих процедура и процеса, неадекватног ууправљања информационим и другим системима, као и услед непредвидивих екстерних догађаја (Закон о банкама, 2015, члан 35).

НБС прописује критеријуме за идентификовање, мерење и процену ризика, као и за управљање ризицима, укључујући и (Закон о банкама, 2015, члан 36):

1) начин израчунавања појединачних показатеља пословања банке у вези са управљањем ризицима и ограничења која се односе на те ризике;
2) начин, форму и рокове извештавања банке о претходним показатељима.

Израда плана опоравка предвиђена је Чланом 36а, где је прописано да је банка дужна да изради и НБС достави план опоравка којим су предвиђене мере које ће банка применити у случају знатног погоршања финансијског стања. Банка је дужна да овај план ажурира најмање једном годишње, а на захтев НБС и чешће (Закон о банкама, 2015, члан 36а, ставови 1 и 2).

Законом је дефинисан садржај плана опоравка (Закон о банкама, 2015, члан 36б) и оцена плана опоравка (Закон о банкама, 2015, члан 36в), где је предвиђено да НБС у року од шест месеци од дана достављања плана опоравка оцењује да ли план испуњава потребне услове. Такође, НБС може да наложи банци да предузме одговарајуће мере, међу којима је и: да преиспита пословну политику и стратегију; извршии промене у начину управљања и да преиспита организациону структуру (Закон о банкама, 2015, члан 36в, став 7, тачка 3, тачка 5 и тачка 6). План опоравка садржи индикаторе на основу којих се утврђује када се одговарајућа мера може предузети (Закон о банкама, 2015, члан 36г).

Банкарска тајна је пословна тајна, регулисано је одељком о тајности података. Банкарском тајном сматрају се (Закон о банкама, 2015, члан 46, став 2):

1) подаци који су познати банци а односе се на личне податке, финансијско стање и трансакције, као и на власништво или пословне везе клијената те или друге банке;
2) подаци о стању и промету на индивидуалним депозитним рачунима;
3) други подаци до којих банка дође у пословању с клијентима.

Банкарском тајном не сматрају се (Закон о банкама, 2015, члан 46, став 3):

1) јавни подаци и подаци који су заинтересованим лицима са оправданим интересом доступни из других извора;
2) консолидовани подаци на основу којих се не открива идентитет појединачног клијнета;
3) подаци о акционарима банке и висини њиховог учешћа у акционарскмо капиталу банке, као и подаци о другим лицима са учешћем у банци и подаци о том учешћу, без обзира на то да ли су они клијенти банке;
4) подаци који се односе на уредност испуњавања обаеза клијената према банци.

Нарушавање пословне тајне, предмет је посебне пажње у заштити информација у банкама, будући да је ова област предмет могућих злоупотреба од стране запослених, одакле банке посебну пажњу треба да посвете овом аспекту заштите.

У ту сврху, банке могу да организују посебне мере заштите, које се огледају у примени контролних техничких мера (ограничења приступа појединим информацијама, којом приликом је потребно поштовати безбедносне принципе да је потребно да запослени приступа одређеним информацијама да би могао да обавља свој радни процес и да је неопходно да је упознат са тим информацијама, енгл: *need to know* и *need to do*; мониторинг приступа појединим информацијама – надлегадање „логовања“, ко је приступао или је покушао да приступи одређеним информацијама), као и нетехничких мера, као што је едукација запослених и подизање свести о безбедности.

Чланом 47 одређено је да банка и чланови њених органа, акционари и запослени у банци, као и спољни ревизори банке и друга лица која због природе посла који обављају имају приступ подацима које је закон одредио као пословну тајну, не могу те податке саопштавати трећим лицима ни користити их противно интересу банке и њених клијената, нити могу трећим лицима омогућити приступ тим подацима. Ова обавезе не престаје ни после престанка статуса на основу ког су остварили приступ подацима. Саопштавање банкарске тајне трећим лицима је могуће уз писано одобрење клијента, осим ако овим или другим законом није друкчије прописано (Закон о банкама, 2015, члан 47) .

У поглављу о заштити информација, ми смо у уводном делу где смо разматрали значај ове области за пословање банака, изнели податак да према једном истраживању област приступања информационом систему банке од стране трећих лица (енгл: *Management of third party access*) спада у топ четири области информационе безбедности у који су банке улагале у току 2018. године.[340]

Изузеци од обавезе чувања банкарске тајне дати су у Члану 48, где је одређено да ова обавеза не постоји ако се подаци саопштавају (Закон о банкама, 2015, члан 48, став 1, тачке 1 до 11):

1) на односу одлуке или захтева надлежног суда;
2) за потребе министарства унутрашњих послова, органа надлежног за борбу против организованог криминала и органа надлежног за спречавање прања новца, у складу са прописима;
3) у вези са имовинским поступком, а на основу одговарајућих захтева и у складу са прописима;
4) у вези са извршењем надлежног органа на имовини клијента банке;
5) регулаторним телима у РС ради обављања послова из њихове надлежности;

[340] Види Графикон број 4: *Области информационе безбедности према улагањима финансијских институција у 2018. години*

6) лицу које су банке основале ради прикупљања података о укупном износу, врсти и ажурности у испуњавању обавеза физичких и правних лица клијената банака;
7) надлежном органу у вези с вршењем контроле обављања платног промета код правних и физичких лица које обављају делатност у складу с прописима којима се уређује платни промет;
8) пореској управи, у складу с прописима којима се уређују послови из њене надлежности;
9) органу надлежном за контролу девизног пословања;
10) на захтев организације за осигурање депозита, у складу са законом којим се уређује осигурање депозита;
11) страном регулаторном телу под условима предвиђеним споразумима о сарадњи закљученим између тог тела и НБС.

Изузетно од одредаба из става 1. овог члана, банка има право да податке који представљају банкарску тајну саопшти истражном судији, јавном тужиоцу и судовима, односно другим органима који врше јавноправна овлашћења искључиво ради заштите својих права, у складу са законом (Закон о банкама, 2015, члан 48, став 2).

Члан 49 предвиђа да НБС, судови и други органи који врше јавноправна овлашћења могу податке до којих су дошли у складу с чланом 47 користити искључиво у сврху за коју су прибављени и не могу их саопштавати трећим лицима нити лицима омогућити да сазнају и користе ове податке, осим у случајевима предвиђеним законом (Закон о банкама, 2015, члан 49).

Објављивање података и информација банке дато је Чланом 51а, где се између осталог наводи да банка није дужна да објављује податке и информације који нису материјално значајни, затим податке и информације чије би објављивање у јавности могло негативно да утиче на конкурентски положај те банке на тржишту, као и податке и информације који представљају банкарску тајну у смислу овог закона (Закон о банкама, 2015, члан 51а, став 2).

Питања спољашње ревизије регулисана су Одељком 6, а за нас је од значаја да Члан 63, који између осталог предвиђа да НБС може банци да наложи ангажовање спољног ревизора ради обављања посебне ревизије, која може да обухвати испитивање појединих пословних процеса (Закон о банкама, 2015, члан 63, став 1).

Члан 64 предвиђа да банке могу, ради унапређења сопственог пословања и усклађивања своје делатности оснивати удружења. Удружење банака има својство правног лица (Закон о банкама, 2015, члан 64, став 1 и став 2).

Глава IV регулише питања организације банке и начин управљања банком, о чему смо у претходном тексту већ говорили кроз давање описа послова Скупштине банке, Управног одбора банке, Извршног одбора банке, и других одбора, као што су: Одбор за праћење пословања банке (Одбор за ревизију), Кредитни одбор и Одбор за управљање активом и пасивом (Закон о банкама, 2015, члан 79).

Одељак 2. одређује систем унутрашњих контрола, функцију контроле усклађености пословања банке и функцију унутрашње ревизије, о чему смо такође већ изнели разматрања у претходном тексту (Закон о банкама, 2015, чланови 82 до 87).

Члан 88 одређује обавезе банке према НБС у смислу обавештавања о отварању филијале или другог организационог облика на територији РС, и то најкасније у року од осам дана од дана њиховог отварања (Закон о банкама, 2015, члан 88).

Глава V одређује контролну функцију Народне банке Србије, где Члан 102 предвиђа да НБС врши контролу бонитета и законитости пословања банке у складу са овим законом и другим законом по којем је НБС надлежна за вршење надзора над пословањем банака (Закон о банкама, 2015, члан 102). Чланом 103, предвиђа се да у поступку непосредне контроле банке могу да учествују и овлашћена лица страног регулаторног тела које контролише, односно надзире пословање чланова исте банкарске групе у којој је и банка, у складу са споразумом о сарадњи закљученим између НБС и тог тела (Закон о банкама, 2015, члан 103, став 3).

Члан 104 предвиђа да је банка дужна да овлашћеним лицима НБС омогући контролу у седишту банке као и свим њеним организационим деловима, а та контрола може да обухвати и информационе технологије (Закон о банкама, 2015, члан 104, став 2). Банка је дужна да овлашћеним лицима стави на увид све пословне књиге и документацију коју та лица захтевају у писаној или електронској форми, као и да им ради вршења контроле рачунарских програма омогући приступ систему базе података који банка користи (Закон о банкама, 2015, члан 104, став 3).

Непосредна контрола се врши у току редовног радног времена, а када је то неопходно због обима и природе контроле, могуће је обавити је и ван радног времена (Закон о банкама, 2015, члан 104, став 4). Овлашћења лица у вршењу контроле могу да (Закон о банкама, 2015, члан 104, став 5, тачке 1 до 4):

1) приступају свим организационим деловима и просторијама банке, уз поштовање безбедносних процедура;
2) захтевају да им се стави на располагање засебна просторија;
3) захтавају копије докумената која су у вези са предметом контроле;
4) непосредно комуницирају с руководиоцем банке и запосленима у банци ради добијања неопходних појашњења.

Из наведеног произилази значај који имају нормативне и организационе мере у заштити информација, будући да банке треба да овај процес организују на такав начин да не буду у супротности са изнетим одредбама, а да са друге стране омогуће одређени степен функционалности заштите информација. У том смислу значај имају интерне процедуре манипулације са интерним документима, приступање информационим системима, а посебно пратеће евиденције.

Члан 112 предвиђа да решење којим се изричу налози и мере за отклањање неправилности утврђених у пословању може да обухвати читав низ мера, између којих и (Закон о банкама, 2015, члан 112):

- да банка смањи трошкове пословања, укључујући износе бонуса и награда за чланове извршног и управног одбора или запосленима;
- да прода имовину, односно акције или удео у подређеном друштву;
- да унапреди систем управљања ризицима;
- да унапреди систем извештавања;
- да унапреди систем унутрашњих контрола, а посебно унутрашње ревизије;
- да разреши дужности члана управног и/или извршног одбора банке, односно друго лице на руководећем положају у банци;
- да затвори једну или више организационих јединица, односно да обустави или ограничи ширење своје организационе мреже;
- да промени управљачку или организациону структуру банке;
- да предузме, односно обустави друге активности.

Из прегледа текста Закона о банкама, у делу који се односи на област заштите информација и на обавезе које банке могу имати по овом основу издвајамо као најважније следеће:

- критичне пословне функције су активности, услуге или послови чији би прекид обављања вероватно довео до угрожавања стабилности финансијског система или поремећаја у пружању неопходних услуга реалном сектору услед величине, тржишног учешћа и повезаности субјекта који их обавља са осталим учесницима у финансијском систему, а нарочито узимајући у обзир могућност да неко други несметано преузме обављање тих активности, услуга или послова (Закон о банкама, 2015, члан 2, став 29);
- подаци који се односе на контролу бонитета и законитости пословања банке и на реструктуирање банке, као и документи који садрже такве податке, а које запослени у НБС, агенцији надлежној за осигурање депозита, министарству надлежном за послове финансија или банци и друга лица на било који начин сазнају у обављању послова у вези са контролом, односно реструктуирањем, одређују се и штите се као тајни подаци са ознаком степена тајности „СТРОГО ПОВЕРЉИВО“, „ПОВЕРЉИВО“ или „ИНТЕРНО“, у складу са законом који уређује тајност података (Закон о банкама, 2015, члан 9б, став 1);
- управљње ризицима је одређено у Члану 28, где се експлицитно наводи да банка идентификује, мери и процењује ризике којима је изложена у свом пословању и управља тим ризицима (Закон о банкама, 2015, члан 28, став 1);
- банка својим актима прописује стратегију и политике за управљање ризицима, стратегију управљања капиталом, процедуре за идентификовање, мерење и процену ризика, као и управљање риицима, у складу с прописима, стандардима и правилима струке, и то (Закон о банкама, 2015, члан 28, став 5):
    - процедуре за идентификовање, мерење и процену ризика;
    - процедуре за управљање ризицима;
    - процедуре којима се обезбеђује контрола и доследна примена свих унутрашњих аката банке у вези са управљањем ризицима;

- процедуре за редовно извештавање органа управе банке и регулаторног тела о управљању ризицима.

– од посебног значаја за предмет истраживања је Члан 29, који наводи врсте ризика, као и да се актима из претходног члана морају обухватити све врсте ризика којима је банка изложена у свом пословању. Посебно су наведене следеће врсте ризика (Закон о банкама, 2015, члан 29):
  - ризик ликвидности;
  - кредитни ризик;
  - каматрни и девизни ризик и остали тржишни ризици;
  - ризици изложености баке према једном лицу или групи повезаних лица;
  - ризици улагања банке у друга правна лица и у основна средства и инвестиционе некретнине банке;
  - ризици који се односе на земљу порекла лица према коме је банка изложена;
  - оперативни ризик, укључујући правни ризик, као и ризик неодговарајућег управљања информационим и других технологијама значајним за пословање банке.
– *Оперативни ризик је могућност настанка негативних ефеката на финансијски резултат и капитал банке услед пропуста у раду запослених, неодговарајућих унутрашњих процедура и процеса, неадекватног ууправљања информационим и другим системима, као и услед непредвидивих екстерних догађаја* (Закон о банкама, 2015, члан 35);
– *Банкарска тајна је пословна тајна*, регулисано је одељком о тајности података (Одељак 4). Банкарском тајном сматрају се (Закон о банкама, 2015, члан 46):
  - подаци који су познати банци а односе се на личне податке, финансијско стање и трансакције, као и на власништво или пословне везе клијената те или друге банке;
  - подаци о стању и промету на индивидуалним депозитним рачунима;
  - други подаци до којих банка дође у пословању с клијентима
– *Нарушавање пословне тајне*, предмет је посебне пажње у заштити информација у банкама, будући да је ова област предмет могућих злоупотреба од стране запослених, одакле банке посебну пажњу треба да посвете овом аспекту заштите. У ту сврху, банке могу да организују посебне мере заштите, које се огледају у примени контролних техничких мера (ограничења приступа појединим информацијама, којом приликом је потребно поштовати безбедносне принципе да је потребно да запослени приступа одређеним информацијама да би могао да обавља свој радни процес и да је неопходно да је упознат са тим информацијама, енгл: *need to know* и *need to do*; мониторинг приступа појединим информацијама – надлегадање „логовања“, ко је приступао или је покушао да приступи одређеним информацијама), као и нетехничких мера, као што је едукација запослених и подизање свести о безбедности. према једном истраживању област приступања информационом систему банке од стране трећих лица (енгл: *Management of third party access*) спада у топ четири области информационе безбедности у који су банке улагале у току 2018. године;

– Члан 104 предвиђа да је банка дужна да овлашћеним лицима НБС омогући контролу у седишту банке као и свим њеним организационим деловима, а та контрола може да обухвати и информационе технологије. Банка је дужна да овлашћеним лицима стави на увид све пословне књиге и документацију коју та лица захтевају у писаној или електронској форми, као и да им ради вршења контроле рачунарских програма омогући приступ систему базе података који банка користи (Закон о банкама, 2015, члан 104).

4.2. Одлука о минималним стандардима управљања информационим системом финансијске институције

Овом одлуком Народна банка Србије утврђује минималне стандарде и услове стабилног и сигурног пословања који се односе на управљање информационим системима у банкама (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 1, став 1).

Акт се односи и на друштва за осигурање, даваоце финанијског лизинга, друштва за управљање добровољним пензијским фондовима, као и на платне институције, институције електронског новца и јавног поштанског оператера у делу пословања који се односи на пружање платних услуга и/или издавање електронског новца.

Одлуком се уређују минимални стандарди за управљање континуитетом пословања и опоравак активности у случају катастрофа у финансијској институцији (Одлука о минималним стандардима урављања информационим системом финансијске институције, 2017, члан 1, став 2).

4.2.1. Основни појмови

Члан 2 дефинише основне појмове, од којих полазећи од предмета истраживања овог рада издвајамо следеће:

Информациони систем је свеобухватни скуп технолошке инфраструктуре (хардверске и софтверске компоненте), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 1).

Ова дефиница како је дата у потпуности одговара нашем приступу у остваривању заштите информација, будући да једнако третира техничке и нетехничке аспекте система, те наглашава да информациони систем, пред техничког дела чине и организација, људи и њихови поступци.

Ресурси информационог система обухватају софтверске компоненте, хардверске компоненте и информациона добра (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 2).

Софтверске компоненте обухватају све типове системског и апликативног софтвера, софтверске развојне алате, као и остали софтвер (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 3).

Хардверске компоненте обухватају рачунарску опрему, комуникациону опрему, медије за чување података као и осталу техничку опрему која служи као подршка функционисању информационог система (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 4).

Ризик информационог система је могућност настанка негативних ефеката на финансијски резултат и капитал, остваривање пословних циљева, пословање у складу с прописима и репутацију финансијске институције услед неадекватног управљања информационим системом или друге слабости у том систему која негативно утиче на њефову функционалност или безбедност, односно угрожава континуитет пословања финансијске институције (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 7).

Контроле су политике, процедуре, праксе, технологије и организационе структуре која се односе на информациони систем, утврђене да би се обезбедило разумно уверење да ће пословни циљеви финансијске институције бити остварени и да ће нежељени догађаји бити спречени или откривени, а могу се разликовати према начину примене (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 8).

У том смислу, документ даље одређује различитте врсте контрола, и то (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 9, тачка 10 и тачка 11):

Према начину примене

- управљачке;
- техничке;
- физичке.

Према намени (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 12, тачка 13 и тачка 14):

- превентивне;
- детективне;
- корективне.

Безбедност информационог система подразумева очување поверљивости, интегритета, расположивости, аутентичности, доказивости, непорецивости и поузданости у информацином систему, да би у даљем тексу документ дефинисао сваки од ових елемената (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 2, тачка 16).

4.2.2. Оквир за управљање информациним системом

Адекватност информационог система је одређена према следећем (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 3):

- ако поседује функционалности, капацитете и перформансе који омогућавају пружање одговарајуће подршке пословним процесима;
- ако обебеђује благовремеме, тачне и потпуне информације значајне за доношење пословних одлука, ефикасно обављање пословних активности и управљање ризицима, односно за сигурно и стабилно пословање финансијксе институције;
- пројектован је са одговарајућим контролама за валидацију података на улазу, у току процеса обраде, као и на излазу из тог система, ради спречавања нетачности и неконзистентности у подацима и информацијама;

Финансијска институција је дужна да обезбеди да сви пословно значајни системи за обраду података, као и системи извештавања, буду интегрални део информационог система (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 3, тачка 3, став 2).

Предвиђена је *обавеза за финансијксе институције* да у складу са стратегијом пословања, као и с природом, обимом и сложеношћу пословања, *донесе стратегију развоја информационог система* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 5).

У складу са овом стратегијом, *финансијска институција је дужна да донесе одговарајуће стратегијске и оперативне планове* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2019, члан 5, став 2).

Свака измена и/или допуна стратегије развоја информационог система мора да се пријави НБС у року од петнаест дана од дана њеног усвајања (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2019, члан 5, став 4).

Члан 6 одређује да је *финансијска институција дужна да*, ради управљања информационим системом, *обезбеди одговарајућу организациону структуру*, с јасно утврђеном поделом послова и дужностима запослених, односно са утврђеним унутрашњим контролама, водећи

рачуна да у таквој организацији не дође до сукоба интереса (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 6).

Финансијска институција је *дужна да обезбеди примену свих унутрашњих општих аката и процедура у вези са информационим системом*, као и да обезбеди да сви корисници овог система буду упознати са садржајем тих аката и процедура, у складу са њиховим овлашћењима, одговорносима и потребама (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 7).

Обавеза је и *да се усвоје и документују одговарајуће методологије* којом ће се утврдити критеријуми, начин и поступци управљања пројектима у вези са информационим системом (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 8).

Потребно је *да се утврде критеријуми, начини и поступци извештавања свог надлежног органа* (унутар финансијске институције) *о функционалности и безбедности информационог система* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 9).

4.2.3. Управљање ризиком информационог система и унутрашња ревизија

Управљање ризиком информационог система је уређено у складу са општим условима и начином управљања ризицима у пословању финансијских институција (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 10).

Унутрашња ревизија информационог система обавља се у складу с прописима којима се уређује пословање финансијских институција (методологијом рада унутрашње ревизије), којом приликом се води рачуна о природи, обиму и сложености пословања, као и о сложености информационог система (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 15).

4.2.4. Безбедност информационог система

Посебна значај има Члан 16, који одређује обавезу *израде политике безбедности информационог система*, као унутрашњег општег акта којим се успоставља оквир за управљање безбедношћу тог система. Политика безбедности информационог система нарочито уређује принципе, начин и процедуре постизања и одржавања адекватног нивоа безбедности, као и овлашћења и одговорности, и мора одражавати промене у окружењу и у

самом информационом систему (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 16).

Управљање безбедношћу информационог система успоставља се као *континуирани процес,* којом приликом је неопходно обезбедити (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2019, члан 17, став 2, тачка 1, тачка 2 и тачка 3):

- поделу послова у вези са безбедношћу информационог система изврши тако да се у унутрашњим актима могу утврдити послови и дужности запослених у вези са безбедношћу;
- одреди кључне запослене задужене за безбедност информационог система;
- укључи у ове послове довољан број запослених који имају одговарајућу стручност и професионално искуство.

Финансијска институција је дужна да ради постизања и одржавања адекватног нивоа безбедности информационог система *успостави одговарајуће контроле* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 18).

Обавеза је, према Члану 19, да се унутрашњим актима *утврде ближи критеријуми, начин и поступци за класификацију информационих добара* према степену осетљивости и критичности (у односу на могуће последице нарушавања поверљивости, интегритета и расположивости). Финансијска институција је *дужна да именује лице, односно лица* запосленена у тој институцији која ће бити *одговорна за управљање информационим добрима, те за класификцију и заштиту добара* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 19, став 2).

Члан 20 говори о обавези спровођења контроле приступа ресурсима информационог система, као и да се с тим у вези успостави *систем управљања корисничким правима приступа.* Под овим се подразумевају процеси (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 20, став 2):

- евидентирање корисника;
- ауторизација;
- идентификација;
- аутентификација;
- надзор над корисничким правима.

Финансијска институција је дужна да се ауторизација заснива на принципу доделе најмањих могућих права приступа који омогућавају ефикасно обављање посла.

Обавеза је да се периодично и по потреби, а најмање једном годишње ревидирају корисничка права приступа (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 20, став 4).

При управљању корисничким правима приступа финансијска институција је дужна да *посебно уреди повлашћени и удаљени приступ информационом систему* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 20, став 5).

Члан 21 одређује обавезу да се на основу резултата процене ризика информационог система *успостави адекватан систем надгледања и генерисања оперативних и системских записа* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 21).

За наведене записе мора да се одреди: време чувања; учесталост, опсег и начин праћења записа. Записи морају да садрже довољно информација ради идентификовања проблема, реконструкције догађаја и откривање неовлашћеног приступа и активности на ресурсима информационог система, као и да обезбеде утврђивање одговорности с тим у вези (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 21, став 2 и став 3).

Предвиђено је да ресурси информатичноког система и други системи који су подршка функционисању информационог система заштити од неовлшћеног физичког приступа (Одлука о минималним стандардима урављања информационим системом финансијске институције, 2017, члан 22). Посебно – финансијска институција је дужна да применом одговарајућих контрола ресурсе информационог система заштити од малициозног програмског кода (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 23).

4.2.5. Управљање континуитетом пословања и опоравак активности у случају катастрофа

Процес управљања континуитетом пословања је предвиђен да се успостави ради обезбеђивања несметаног и континуираног функционисања свих својих значајних система и процеса, као и ограничавања губитака у ванредним ситуацијама (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 24).

Управљање континуитетом пословања треба да је засновано на анализи утицаја на пословање и на процене ризика, које нарочито обухватају (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 25, став 1, тачке 1 до 5):

1) утврђивање ресурса и система потребних за одвијање појединачних пословних процеса, као и њихове међузависности и повезаности;

2) процену ризика у вези с појединачним пословним процесима, укључујући и вероватноћу настанка нежељених догађаја и њихов потенцијални утицај на континуитет пословања, финансијско стање и репутацију финансијске институције
3) утврђивање прихватљивих нивоа ризика и техника за ублажавање идентификованих ризика
4) утврђивање најдужег прихватљивог прекида (МАО) појединачних пословних процеса
5) утврђивање критичних/кључних пословних процеса и активности

Финансијска институција мора да усвоји стратегију опоравка коју ће применити у случају прекида пословања, а која мора да садржи: приоритете опоравка пословног процеса, као и ресурса и система потребних за њихово одвијање и – циљне нивое активности (SDO); циљна времена опоравка (RTO) и циљне тачке опоравка (RPO) (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 25, став 2, тачке 1 до 4).

Управни одбор банке, односно надлежни орган финансијске институције, дужан је да донесе план континуитета пословања (енгл: *Business Continuity Plan*) и план опоравка активности у случају катастрофа (енгл: *Disaster Recovery Plan*) (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 26).

Одређено је да *План континуитета пословања мора да садржи* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 26, став 2, тачке 1 до 4):

1) опис процедура у случају прекида пословања;
2) ажуран списак свих ресурса неопходних за поновно успостављање континуитета пословања
3) податке о тимовима који ће бити одговорни за поновно успостављање пословања у случају настанка непредвиђених догађаја и податке о именованим члановима тих тимова, укључујући и њихове јасно утврђене дужности и одговорности, као и план унутрашњих и спољних линија комуникације;
4) резервну локацију.

План опоравка активности у случају катастрофа мора да садржи (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 26, став 3, тачке 1 до 4):

1) процедуре за опоравак информационог система кад наступе катастрофални догађаји
2) приоритете опоравка ресурса информацоног система
3) податке о тимовима који ће бити одговорни за опоравак информационог система и о именованим члановима тих тимова, укључујући и њихове јасно утврђене дужности и одговорности;

4) резервну локацију за опоравак информационог система, односно локацију резервног рачунарског центра.

Обавеза је да финансијска институција ове документе има ажурно, укључујући све релеватне промене које утичу на активности, производе, процесе и системе, уважавајући промене окружења. С тим у вези, потребно је периодично, а *најмање једном годишње, тестирати наведене планове, као и документовати резултате тестирања и обезбедити извештавање надлежног органа о истом* (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 26, став 6). За спровођење свега наведеног одговоран је извршни одбор банке, односно надлежни орган друштва који води послове (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 26, став 7).

При управљању континуитетом пословања морају се узети у обзир и активности поверене трећим лицима, у зависности од услуга тих лица (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 27).

Уколио наступе околности које захтевају примену плана континуитета пословања и плана опоравка активности у случају катастрофа, о истом се мора обавестити НБС, најкасније наредног дана (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 28).

Процес управљања инцидентима подразумева претходно наведено о обавештавању НБС, и то (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2019, члан 29, став 2, тачке 1 до 3):

1) ако је настао услед нарушавања функционалности ресурса информационог система – одмах по утврђивању околности о настанку инцидента;
2) ако је настао као последица нарушавања безбедности информационог система – одмах по сазнању о инциденту;
3) ако је настао код пружаоца услуге, а имао је илои је могао имати значајан утицај на информациони систем финансијске институције – одмах по утврђивању околности о настанку тог инцидента.

Одлуком су утврђени и друге обавезе у вези са извештавањем НБС, а у вези са континуитетом извештавања (ако криза траје), достављања завршног извештаја о догађају и друго.

Чланом 29а *придвиђено је тромесечно извештавање НБС о инцидентима који су повезани са злоупотребом осетљивих података корисника финансијских услуга*, неодобреним платним трансакцијама, злоупотребом, крађом или губитком платних инструмената, укључујући коришћење техничких манипулација на банкоматима (АТМ), преварним радњама и злоупотребама корисника финансијских услуга, злоупотребама фактора аутентификације и система за аутентификацију и сл., а који нису имали директан утицај на

информациони систем (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2019, члан 29а, став 1).

Такође, финансијска институција је дужна *да успоставља процес управљања резервним копијама података, и с тим у вези да утврди детаљне процедуре и одговорности*. Управљање резервним копијама података, у циљу поновног успостављања пословних процеса у оквиру циљног времена опоравка, мора да обухвати поступке (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 30, став 2):

- израде копије података,
- чувања копије података,
- тестирања копија, и
- опоравка података и софверских компонената.

Најмање једна (ажурна и комплетна) копија података мора бити адекватно ускладиштена на одговарајућој удаљености од примарне локације, а на основу резултата процене ризика информациног система и узимања у обзир принципа да се избегава утицај истих ризика на обе локације (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 30, став 4).

Резервни рачунарски центар мора да је адекватно опремљен, функионалан и да има одговарајући ниво безбедности, уз узимање у обзир претходно наведеног о удаљености локација (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 31).

4.2.6. Развој и одржавање информационог система

Финансијска институција је дужна да успостави процес развоја информационог система у складу с релевантним променама унутар финансијске институције и у окружењу, као би се обезбедила континуирана адекватност тог система (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 32).

Обавеза је да се у складу са усвојеном стратегијом развоја информационог система и методологијом управљања пројектима, успостави и документује процес тог развоја, који обухвата анализу, пројектовање, програмирање, тестирање и увођење у продукцију. Потребно је на одговарајући начин раздвојити развојно, тестно и продукционо окружење (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 33).

Члан 36 између осталог обавезује да се све промене хардверских и софтверских компоненти, укључујући и нове компоненте и системе, буду тестирани и одобрени пре пуштања у рад, као и да се утврди план враћања на претходно стање. Унутрашњим општим

актом се уређује процес управљања хитним променама свих компоненти информационог система (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 36).

Када се планира миграција података на нови систем главних пословних апликација (енгл: *core businesss application*), или у други рачунарски центар, обавеза је пријављивања ове активности НБС најкасније тридесет дана пре почетка тестирања планираног у вези с том миграцијом (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2019, члан 37, став 5).

Истим чланом је регулисана обавеза враћања на стање пре миграције података због статусне промене, о чему је банка дужна да обавести НБС најкасније наредног радног дана од дана када је започела миграцију података, и то најкасније сат пре почетка периода утврђеног Дневним терминским планом рада RTGS платног промета НБС за извршење налога за пренос у том систему.

Финансијска институција је дужна да обезбеди адекватно, континуирано стручно оспособљавање и обучавање запослених за коришћење информационих система и очување његове безбедности и функционалности (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 39).

4.2.7. Поверавање активности у вези са информационим системом трећим лицима

Под поверавањем активности трећим лицима, у вези са информационом системом финансијске институције, сматрају се све активности које обухватају обраду, чување и/или приступ подацима којима располаже финансијска институција а односе се на њено пословање, као и активности развоја и/или одржавања главних пословних апликација (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 40, став 2). Ово подразумева и поверавање активности лицима повезаним с финансијском институцијом имовинским и управљачким односима (лица са учешћем, чланице групе друштва којој та институција припада и др.) која послују у РС или у иностранству.

Под поверавањем активности не сматра се коришћење стандардизованих сервиса, као што су SWIFT, Bloomberg, Reuters и друго, или телекомуникационих услуга, као ни набавка софвера који је као готово решење комерцијално дуступан тржишту (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 40, став 4).

Пре доношења одлуке о сваком појединачном поверавању активности финансијска институција је дужна да (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 42):

1) изврши детаљну анализу способности добављача за пружање услуга, финансијско стање и пословну репутацију;
2) утврди да ли прописи државе или држава где пружалац услуге послује омогућавају НБС несметано вршење контроле пословања у делу који се односи на обављање поверених активности или је у вези са тим активностима;
3) процени могуће потешкоће и време потребно за избор другог пружаоца услуга, или могућност наставка обављања тих активности унутар финансијске институције у случају престанка пружања уговорених услуга, као и да с тим у вези донесе одговарајућу излазну стратегију. Она мора да садржи списак мера и активности које је потребно предузети, као и динамику њиховог спровођења од тренутка престанка пружања уговорених услуга до избора другог пружаоца услуга или потпуног успостављања процеса обављања тих активности унутар финансијске институције.

При доношењу одлуке о поверавању активности финансијска институција нарочито процењује утицај поверавања активности на:

1) континутитет пословања и репутацију финансијске институције;
2) трокове, финансијски резултат, ликвидност и солвентност финансијске институције;
3) ризични профил финансијске институције;
4) квалитет услуга које финансијска институција пружа клијентима.

Обавеза је да финансијска институција обезбеди да се поверавањем активности на угрози безбедност или функционалност информационог система, као и да подаци финансијске институције остану у њеном поседу (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 44).

Поверавање активности, односно промена пружаоца услуга мора да се пријави НБС најкасније тридесет дана пре закључења уговора о поверавању активности (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2013, члан 45).

Финансијска институција одговара у целини за активности које је поверила пружаоцу услуга. У том смислу, она је дужна да континуирано врши надзор над пруженим услугама, као и проверу квалитета пружених услуга у вези с повереним активностима (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2013, члан 48).

4.2.8. Електронске услуге

Финансијска институција која је пружалац електронских услуга дужна је да, као саставни део управљања ризиком информационих система, успостави процес управљања ризицима

који произилазе из пружања електронских услуга (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 49).

Приком пружања ових услуга, обавеза је примена безбедних и ефикасних метода за проверу и потврду идентитета и овлашћења лица, процеса и система (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 50, став 1).

Пружалац је дужан да корисницима обезбеди аутентификацију која укључује комбинацију најмање два међусобно зависна елемента за потврђивање корисничког идентитета. Изузетно, може се применти коришћење аутентификација са једним елементом, и то у случајевима (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 50, став 2 и став 3):

1) плаћања мале новчане вредности;
2) плаћање према предефинисаним примаоцима;
3) пренос новчаних средстсава између два рачуна истог корисника и код истог пружаоца електронских услуга;
4) преног електронског новца у оквиру једног пружаоца електронских услуга;
5) других трансакција које се на основу анализе ризика процене као нискоризичне.

Одређено је да приликом коришћења једнократних лозинки ради аутентификације (енгл: *One Time Password*), пружалац електронских услуга је дужан да обезбеди да временско важење те лозинке буде ограничено на период који је потребан за обављање аутентификације, као и да утврди највећи број неуспешних покушаја пријаве на систем, у ком случају се приступ блокира трајно или привремено. Такође, обавеза је да се утврди најдуже могуће време без активности корисника на систему, након којег долази до аутоматског одјављивања корисника из система (Одлука о минималним стандардима управљања информационим системом финансијске институције, 2017, члан 51, став 2, став 3 и став 4).

4.3. Одлука о управљању ризима банке

Народна банка Србије прописује ближе услове и начин идентификације, мерења и процене ризика којима је банка изложена у свом пословању, осим ризика усклађености пословања (Одлука о управљању ризицима банке, 2017, члан 1).

Одређене су врсте ризика којима је банка изложена, којом приликом се дају ближа објашњења шта се сматра под поједином врстом ризика (Одлука о управљању ризицима банке, 2017, члан 3) и то:

1) ризик ликвидности,

2) кредитни ризик, укључујући и резидуални ризик, ризик смањења вредности потраживања, ризик измирења/испоруке, као и ризик друге уговорне стране. *Резидулани ризик* је могућност настанка негативних ефеката на финансијски резултат и капитал банке услед тога што су технике ублажавања кредитног ризика мање ефикасне него што се очекује, или њихова примена недовољно утиче на умањење ризика којима је банка изложена. *Ризик смањења вредности потраживања* јесте могућност настанка негативних ефеката на финансијски резултат и капирал банке по основу смањења вредности откупљених потраживања услед готовинских или неготовинских обавеза претходног повериоца према дужнику. *Ризик измирења/испоруке* је могућност настанка негативних ефеката на финансијски резултат и капитал банке по основу неизмирених трансакција или услед неизвршавања обавезе друге уговорне стране по трансакцијама слободне испоруке на уговорени датум измирења/испоруке. Ризик друге уговорне стране јесте могућност настанка негативних ефеката на финансијски резултат и капитал банке услед неизмирења обавезе друге уговорне стране у трансакцији пре коначног поравњања новчаних токова трансакције, односно измирења новчаних обавеза по тој трансакцији;
3) каматни ризик;
4) девизни ризик и остали тржишни ризици;
5) ризик концентрације, који посебно укључује ризике изложености банке према једном лицу или групи повезаних лица;
6) ризици улагања банке;
7) ризици који се односе на земљу порекла лица према коме је банка изложена (ризик земље);
8) *оперативни ризик*, који посебно укључује правни ризик, где је он одређен као ризик настанка негативних ефеката на финансијски резултат и капитал банке по основу судских или вансудских поступака у вези с пословањем банке (облигациони односи, радни односи и сл);
9) ризик усклађености пословања банке, који представља могућност настанка негативних ефеката на финансијски резултат и капитал банке услед пропуштања усклађивања пословања са законом и другим прописом, стандардима пословања, процедурама о спречавању прања новца и финансирања теротизма и другим процедурама, као и с другим актима којима се уређује пословање банака, а посебно обухвата ризик од санкција регулаторног тела, ризик од финансијских губитака и репутациони ризик;
10) ризик од прања новца и финансирања тероризма;
11) стратешки ризик, који представља могућност настанка негативних ефеката на финансијски резултат или капитал банке услед непостојања одговарајућих политика и стратегија, те њиховог неадекватног спровођења, као и услед промена у окружењу у коме банка послује или изостанка одговарајућег реаговања банке на те промене;
12) други ризици.

На основу изнетог можемо да закључимо да је *по питању заштите информација банка изложена по више врста ризика*, као што су оперативни ризик, ризик усклађености пословања банке, ризик од санкција регулаторног тела, ризик од финансијског губитка, репутациони ризик и стратешки ризик.

Систем управљања ризицима обухвата (Одлука о управљању ризицима банке, 2017, члан 4):

- стратегију, политике и процедуре за управљање ризицима, односно за идентификовање, мерење, процену, праћење, контролу и ублажавање ризика и извештавање о њима;
- унутрашњу организацију, односно организациону структуру банке;
- ефективан и ефикасан процес управљања свим ризицима којима је банка изложена или може бити изложена у свом пословању;
- адекватан систем унутрашњих контрола;
- одговарајући информациони систем;
- акедватан процес интерне процене адекватности капитала.

4.3.1. Стратегија, политике и процедуре

Стратегију за управљање ризицима чини један или више докумената којима се уређује јединствено и доследно управљање ризицима банке на дугорочној основи и којима је одређен однос банке према ризицима којима је изложена или може бити изложена у свом пословању, укључујући и ризике који произилазе из макроекономског окружења у коме банка послује (Одлука о управљању ризицима банке, 2017, члан 5).

Стратегија треба да буде усклађена с пословном политиком и стратегијом банке.

Стратегија нарочито садржи (Одлука о управљању ризицима банке, 2017, члан 6):

- преглед и дефиниције свих ризика којима је банка изложена или може бити изложена;
- дугорочне циљеве утврђене пословном политиком и стратегијом банке, као и склоност ка ризицима одређену у складу с тим циљевима;
- основна начела преузимања ризика и управљања ризицима;
- основна начела процеса интерне процене адекватности капитала банке.

Политике за управљање ризицима чине један или више докумената банке којима се нарочито уређује (Одлука о управљању ризицима банке, 2017, члан 7):

- начин организовања процеса управљања ризицима банке и јасно разграничење одговорности запослених у свим фазама тог процеса;
- начин процене ризичног профила банке и методологије за идентификовање и мерење ризика, односно процену појединачних ризика;

- мере за ублажавање појединачних ризика и правила за примену тих мера;
- начин праћења и контроле појединачних ризика и успостављање система лимита банке;
- начин одлучивања и поступања код прекорачења успостављања лимита, као и дефинисање изузетних околности у којима је одобравање то гпрекорачења могуће у законским оквирима;
- принцип функционалности система унутрашњих контрола банке, начин и методологија за спровођење процеса интерне процене адекватности капитала банке;
- оквир и учесталост стрес тестирања, као и поступање у случајевима неповољних резултата стрес тестова.

Банка дужна да, на основу стратегије и политика за управљање ризицима, усвоји и примењује процедуре за идентификовање, мерење, односно процену ризика којима је изложена, као и за управљање тим ризицима (Одлука о управљању ризицима банке, 2017, члан 8).

Процедуре за мерење, односно процену ризика нарочито садрже квантитативне и/или квалитативне методе на основу којих банка може благовремено уочити промене свог ризичног профила, укључујући и настанак нових ризика. Процедуре за управљање ризицима нарочито садрже опис поступака за ублажавање ризика, као и опис поступака за праћење и контролу ризика (Одлука о управљању ризицима банке, 2017, члан 8, став3).

Банка је дужна да наведене акте приспитује најмае једном годишње, а ако настану значајне промене у ризичном профилу банке и чешће, као и да из, по потреби, мења.

4.3.2. Унутрашња организација (организациона структура)

Банка је дужна да успостави такву унутрашњу организацију, односно организациону структуру којом ће активности управљања ризицима (енгл: *middle office*) и активности подршке (енгл: *back office*) функционално и организационо одвојити од преузимања ризика (енгл: *frong office*), с јасно утврђеном поделом послова и дужности запослених којом се спречава сукоб интереса (Одлука о управљању ризицима банке, 2017, члан 9).

Обавеза функционалног и организационог одвајања подразумева да овлашћења и одговорности за послове који се односе на управљање ризицима, односно активности подршке не могу бити поверени оном члану извршног одбора коме су поверена овлашћења и одговорности за послове који се односе на преузимање ризика (Одлука о управљању ризицима банке, 2017, члан 8, став 2).

4.3.3. Процес управљања ризицима

Банка је дужна да успостави ефективан и ефикасан процес управљања ризицима, који обухвата ублажавање, праћење и контролу ризика којима је банка изложена или може бити изложена а које је идентификовала и измерила, односно проценила. У оквиру процеса управљања ризицима банка је дужна да (Одлука о управљању ризицима банке, 2017, члан 13):

- благовремено, свеобухватно и континуирано идентификује ризике којима је у свом пословању изложена или може бити изложена, као и да анализира узроке који доводе до настанка ризика;
- редовно мери, односно процењује ризике које је идентификовала у свом пословању, при чему поступци мерења, односно процене ризика морају обухватити одговарајуће квантитативне и/или квалитативне методе на основу којих банка може благовремено уочити промене свог ризичног профила, укључујући и настанак нових ризика;
- одреди јасне критеријуме за одлучивање и поступке за ублажавање ризика који се односе на преузимање, диверсификацију, пренос, смањење и/или избегавање ризика, имајући у виду ризични профил и склоност банке ка ризицима, као и њену толеранцију према ризицима;
- на одговарајући начин документује праћење и контролу ризика, односно учесталост и начин праћења ризика којима је изложена, као и праћење и контролу лиита у оквиру успостављеног система лимита.

4.3.4. Систем унутрашњих контрола

Систем унутрашњих контрола представља скуп процеса и процедура успостављених ради адекватне контроле ризика, праћења ефикасности и ефикасности пословања, поузданости финансијских и осталих података и информација банке, као и њихове усклађености с прописима, унутрашњим актима и пословним стандардима. Систем унутрашњих контрола банке обухвата (Одлука о управљању ризицима банке, 2017, члан 15, став 1 и став 2);

- одговарајуће контролне активности, које спроводе извршни одбор банке, лица одговорна за управљање ризицима и запослени у банци;
- редовну процену адекватности, поузданости и ефикасности система управљања ризицима, коју врши унутрашња ревизија.

Банка дужна да обезбеди да унутрашње контроле буду саставни део свакодневних активности запослених, као и да они треба да разумеју сврху и значај ових контрола (Одлука о управљању ризицима банке, 2017, члан 16).

4.3.5. Информациони систем

За нас је од посебне важности обавеза која је дата банкама да усвоји и примењује стратегију развоја информационог система и политику информационог система. Стратегијом развоја информационог система банка обезбеђује да тај систем увек буде у складу с природом, обимом и сложеношћу активности банке (Одлука о управљању ризицима банке, 2017, члан 17, став 1 и став 2).

Политика сигурности информационог система нарочито се односи на (Одлука о управљању ризицима банке, 2017, члан 17, став 3):

1) начин обезбеђивања сигурности овог система;
2) принципе и процедуре за обезбеђивање:
   - поверљивости података;
   - интегритета;
   - доступности података овлашћеним лицима кад је то потребно.
3) поделу послова и дужности у вези са информационом технологијом, подацима из информационог система и пратећом документацијом.

Банка је дужна да обезбеди да рачуноводствени систем, други системи за обраду података, као и систем извештавања, буду интегрални део информационог система банке (Одлука о управљању ризицима банке, 2017, члан 18).

4.3.6. Систем извештавања о ризицима

Предвиђено је да је банка дужна да успостави систем извештавања о ризицима који ће релевантним запосленима на свим нивоима у банци обезбедити благовремене, тачне и добољне детаљне информације које су неопходне за доношење пословних одлука и ефикасно управљање ризицима, односно за сигурно и стабилно пословање банке (Одлука о управљању ризицима банке, 2017, члан 19).

У акту су наведене информације које нарочито обухватају систем ивешвања, где се наводе као обавезне информације о ризицима који настају као последица поверавања активности банке трећим лицима.

4.3.7. Стрес тестирање

Одлука предвиђа да редовно, а најмање једном годишње, банка спроводи стрес тестирање на нивоу појединачно материјално значајних ризика којима је изложена (Одлука о управљању ризицима банке, 2017, члан 19а).

Под стрес тестирањем подразумева се процена потенцијалних ефеката специфичних догађаја и/или промене више фактора ризика на капитал, ликвидност и финансијски резултат банке. Стрес тестирање се може спроводити (Одлука о управљању ризицима банке, 2017, члан 19а, став 2):

1) анализом осетљивости, где се процењују ефекти промене одређеног фактора ризика;
2) сценарио-анализом, где се процењују истовремене промене више фактора ризика.

Могуће је користити и обрнуто стрес тестирање, као облик где се полази од дефинисања исхода, где се идентификују сценарији или комбинација сценарија који могу довести до тог исхода (Одлука о управљању ризицима банке, 2017, члан 19а, став 3).

Банка је дужна да унутрашњим актима обухвати (Одлука о управљању ризицима банке, 2017, члан 19а, став 5):

1) коришћење различитих облика стрес тестирања;
2) учесталост спровођења различитих врста стрес тестова;
3) овлашћења, обавезе и одговорности у процесу стрес тестирања;
4) детаљан опис методологија стрес тестирања
5) претпоставке које се користе у стрес тестирању
6) информациони систем и систем извештавања о ризицима који представљају подршку процесу стрес тестирања.

4.3.8. Управљање оперативним ризицима банке

Раније смо већ навели дефиницију оперативних ризика, као најзначајније групе ризика која се односи на безбедност, где су груписани пропусти запослених, неодговарајуће унутрашње процедуре и процеси, неадекватно управљање информационим и другим системима у банци, као и непредвидљиви екстерни догађаји. Напоменули смо и да оперативни ризик укључује правни ризик.

Банка је дужна да идентификује и процени догађаје и изворе због који могу настати губици у вези са оперативним ризицима, узимајући у обзир све значајне унутрашње и спољне факторе (Одлука о управљању ризицима банке, 2017, члан 65).

Изложеност оперативном ризику процењује се узимајући у обзир могућност, односно учесталост настанка тог ризика, као и његов потенцијални утицај на банку, с посебним

освртом на догађаје за које је мало вероватно да ће настати али могу изазвати велике материјалне губитке (Одлука о управљању ризицима банке, 2017, члан 66).

Посебно се процењује да ли је овом ризику изложена по основу увођења нових производа, активности, процеса и система, а банка процењује и активности чије је обављање поверила трећим лицима.

За наш предмет итраживања од посебног је значаја обавеза управног одбора банке да усвоји план континуитета пословања (енгл: *Business Continuity Plan – BCP* план), као и план опоравка активности у случају катастрофа (енгл: *Disaster Recovery Plan – DRP* план) (Одлука о управљању ризицима банке, 2017, члан 68).

Ови планови омогућавају несметано и континуирано функционисање свих значајних система и процеса банке, као и ограничавање губитака у ванредним ситуацијама.

Извршни одбор банке је одговоран за (Одлука о управљању ризицима банке, 2017, члан 68, став 2):

- спровођење *BCP* и *DRP* планова, као и за обуку и упознавање запослених с њиховом улогом и одговорностима у случају наступања ванредних ситуација;
- измене *BCP* и *DRP* планова, у складу с пословним променама, укључујући и промене у производима, активностима, процесима и системима, с променама у окружењу, као и с пословном политиком и стратегијом банке;
- редовно тестирање *BCP* и *DRP* планова, уз адекватну документованост резултата тестирања и њихово укључивање у извештавање управног одбора банке.

Банка је ради спровођења континуитета пословања дужна да (Одлука о управљању ризицима банке, члан 69):

1) уврди кључне пословне активности (укључујући и оне које је поверила трећим лицима), ресурсе и системе потребне за обављање пословних процеса, као и њихову међузависност и повезаност;
2) утврди критично време за поједине пословне процесе, односно период после ког је неопходно поново успоставити ове процесе;
3) процени ризике који могу довести до прекида континуитета пословања банке и утицати на финансијско стање и/или репутацију банке;
4) процени вероватноћу настанка и значаја утицаја претходно наведених ризика
5) усвоји стратегију опоравка у којој ће утврдити следеће основне циљеве које треба да оствати у случају прекида пословања:

    - приоритете опоравка;
    - прихватљив ниво активности;
    - прихватљив ниво ризика и технике за ублажавање идентификованих ризика;

- време опоравка, односно период до поновног успостављања редовних пословних процеса, који би требали да буду краћи у односу на критично време.

BCP план садржи (Одлука о управљању ризицима банке, 2017, члан 70):

- опис процедура у случају прекида пословања;
- списак свих ресурса неопходних за поновно успостављање континуитета послвоања;
- именовање тимова који ће бити одговорни за поновно успостављање пословања у случају настанка непредвиђених догађаја;
- јасно утврђене дужности и одговорности тимова и појединих чланова тих тимова, као и план интерних и екстерних линија комуникације;
- резервну локацију за случај прекида пословања и немогућности поновног успостављања пословних процеса на примарној локацији;

DRP план обезбеђује могућност поновног успостављања опоравка система информационе технологије какав је био пре прекида пословања, укључујући и процедуре израде и чувања резервних копија свих података потребних за поновно успостављање процеса који подржавају тај систем. Овај план садржи нарочито (Одлука о управљању ризицима банке, 2017, члан 71):

- процедуре за опоравак система информационе технологије у случају наступања катастрофалних догађаја;
- приоритете оправка ресурса информационе технологије;
- именовање тимова који ће бити одговорни за опоравак система информационе технологије;
- јасно утврђене дужности и одговорности тимова и појединих чланова тих тимова;
- резервну локацију за опоравак система информационе технологије.

Банка је дужна да у случају настанка околности који захтевају примену *BCP* и *DRP* планова обавести НБС, и то у року од једног дана, о свим релевантним чињеницама и околностима које се на то односе.

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

Управљање ризицима мора да обухвати и активности које је банка поверила трећим лицима, којом приликом треће лице обавља ту активности као претежну делатност (Одлука о управљању ризицима банке, 2017, члан 74). То подразумева активности дефинисане у Закону о банкама, као што су: депозитни, кредитни, девизни, мењачки послови, послови платног промета, издавање платних картица и друго.

Под овим услугама не сматрају се стандардизоване услуге као што су услуге у вези коришћења телекомуникација, услуге оглашавања, услуге чишћења, услуге испитивања тржишта и набавка робе (Одлука о управљању ризицима банке, 2017, члан 74, став 2).

Банке је дужна да, када намерава да повери трећем лицу активности чије је извршење значајно за обезбеђивае континуитета пословања банке, обезбеди континуитет тих функција на један од следећих начина (Одлука о управљању ризицима банке, 2017, члан 75).

1) обавезивањем тог лица да обавља активности у свим ситуацијама у којим је потребно обезбедити континуитет критичних функција банке;
2) уговором са алтернативним добављачем;
3) детаљним планом обезбеђивања континуитета обављања критичних фукција употребом интерно расположивих ресурса.

Пре доношења одлуке о сваком појединачном поверавању активности, банка је дужна да (Одлука о управљању ризицима банке, 2017, члан 75а):

1) изврши детаљну анализу потенцијалног пружаоца услуге (способност пружања услуге, финансијско стање и пословна репутација);
2) утврди да ли прописи државе или држава у којима пружалац услуга послује омогућавају НБС несметано вршење непосредне контроле тог пословања у делу који се односи на поверене активности или је у вези с њима;
3) процени могуће потешкоће и време потребно за наставак обављања поверених активности у случају изненадног престанка њиховог обављања и време потребно за избор другог пружаоца услуга

Предвиђено је да банка има обавезу да најкасније тридесет дана пре закључења уговора о предметном о томе обавести НБС и уз то достави документацију која је састави део Одлуке (Одлука о управљању ризицима банке, 2017, члан 76).

4.3.10. Ризик од прања ноца и финансирања тероризма

Одлука наводи да је ризик од прања новца и финансирања тероризма ризик могућег настанка негативних ефеката на финансијски резултат, капитал или репутацију банке услед коришћења банке у сврху прања новца и/или финансирање тероризма (Одлука о управљању ризицима банке, 2017, члан 78а).

Овај ризик настаје нарочито као последица пропуштања усклађивања пословања банке са законом, прописима и унутрашњим актима банке којима се уређује спречавање прања новца и финансирања тероризма, односно као поседица међусобне неусклађености њених

унутрашњих аката којима се уређује поступање банке и њених запослених у вези са спречавањем прања новца и финансирање тероризма.

За потребе идентификовања, мерења и процене ризика од прања новца и финансирања тероризма, банка је дужна да изради анализу ризика за сваку групу или врсту клијената, која најмање обухвата (Одлука о управљању ризицима банке, 2017, члан 78в):

1) утврђивање прихватљивости клијента према степену ризика од прања новца и финансирања тероризма;
2) утврђивање категорије ризика клијента према факторима ризика у односу на ризик прања новца и финансирања тероризма;
3) познавање клијента и редовно праћење његовог пословања
4) одређивање производа или услуга које банке неће пружати клијентима одређене категорије ризика.

Банка је дужна да при процени ове врсте ризика нарочито узме у обзир сложеност организационе структуре банке, број запослених задужених за непосредно обављање послова у вези са спречавањем прања новца и финансирања тероризма у односу на укупан број запослених, број запослених који су у непосредном контакту с клијентима, начин организације послова и одговорности, као и динамику запошљавања нових кадрова и квалитет обуке.

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

Несуњиво је да су данас економски системи међусобно повезани, што значи и да су међусобно осетљиви и да имају утицај једни на друге.

Банке и банкарске организације имају истакнуту улогу у тим односима, будући да су од великог значаја за економију једне земље или региона, одакле произилази интерес за међународном координацијом банкарских политика.

Ми смо у претходним поглављима истакли значај који имају политике банака на уређење области заштите информација у њима, будући да су на њима конципирани стандарди, политике, правила, процедуре и други интерни акти ових организација, одакле у коначном имамо нормативни оквир уређења заштите информација у банкама и финансијским институцијама.

Полазећи од наведеног, природно је да у нашем раду имамо интересовање за истраживање инструмената међународне координације банкарских политика, који се конституишу преко кодекса стандарда, правила, директива, међународних споразума и међународних клубова и нтеграција, којом приликом имамо свест и о потребном нивоу политичке сарадње између држава, што у нашем раду није предмет истраживања, али смо свесни и ове условљености.

У теоријским радовима постоји сагласност о значају Базелског комитета у том смислу, који представља механизам међународне координације банкарских политика. Његово деловање има неколико димензија: хармонизацију стандарда за пословање банака, надзор над радом бананка и сарадњу са другим међународним механизмима за координацију банкарских политика.[341]

5.1. Базелски споразуми

Базелски комитет за надзор над банкама основан је седамдесетих година прошлог века, и тада су национални органи за надзор над банкама неколико развијених земаља оценили да међународно пословање банака, потребе координације њихових политика и међузависност националних банкарских система, захтева координацију и даље активности у том смислу. Чланови, оснивачи Базелског комитета били су гувернери централних банака земаља OECD (Организација за економску сарадњу и развој[342]), односно Групе 10[343] и Гувернер Централне банке Швајцарске, а све у оквиру Банке за међународна поравнања (БИС).[344]

Банка за међународна поравнања (енгл: *Bank for International Settlements – BIS*) је најстарија међународна финансијска организација, основана 17. маја 1930. године у Базелу. Банка је акционарско друштво са ограниченом одговорношћу, у власништву и под управом централних банака, које имају право гласа у складу са бројем акција које поседују. Основна улога БИС-а је да подстиче међународну монетарну и финансијску сарадњу и посредује у финансијским трансакцијама између централних банака. Народна банка Краљевине Југославије је била чланица од 1931. године. Учешће СФРЈ је замрзнуто 1992. године, а СР Југославија је 2001. године обновила чланство. НБС је 2009. године је наставила чланство са 2.920 акција. У мају 2012. године НБС је постала члан Мреже за унапређење управљања централним банкама у оквиру БИС-а.[345]

Владе не учствују у Безелском комитету, већ су чланови њихови монетерни органи и органи надзора над банкама.

Основна идеја овог тела је да стандарди и смернице које утврђује буду примењивани од стране надзорних органа учесника, односно да представљају необавезујуће конвенционалне споразуме за друге земље. Потребе међународне координације банкарских политика, због квалитета и садржаја правила које је Базелски комитет донео, учинели су да су акта

[341] Огњановић, В.: *Међународна сарадња банкарских политика*, часопис Банкарство, 2005. година, доступно на: https://www.ubs-asb.com/Portals/0/Casopis/2005/5_6/UBS-Bankarstvo-5-6-2005-Ognjanovic.pdf
[342] Доступно на: http://www.oecd.org/
[343] Чланови Групе 10, организације за координацију у области економије, монетарне и фискалне политике су: Белгија, Канада, Француска, Немачка, Италија, Јапан, Холандија, Шведска, Велика Британија и САД, доступно на: https://stats.oecd.org/glossary/detail.asp?ID=7022
[344] *Ibid*
[345] Доступно на: https://www.nbs.rs/internet/cirilica/40/40_7/index.html

Базелског комитета опште прихваћен модел међународне координације банкарских политика.[346]

Главни циљеви Базелског комитета су: јачање здравља и стабилности све више међузависног међународног банкарског система и − смањење постојећих неједнакости у конкуренцији између банака основаних у различитим земљама.

Поред ове институције (и БИС-а), у области међународне банкарске сарадње допринос дају и Међународни монетарни фонд (Кодекс о транспарентности у монетарној и финансијског политици из 1998. године), ЕУ (са више својих директива), Париски клуб, Лондонски клуб и друго.[347]

Базелски споразум је више пута мењан и допуњиван, а данас постоје: Базелски споразуми I, II и III, где нашу пажњу, полазећи од предмета истраживања, посебно привлачи Базел II, будући да он третира оперативни ризик, а претходно смо видели његов значај на област заштите информација у банкама и финансијским институцијама.

Базел I споразум је имао за сврху увођење јединственог начина за израчунавање адекватности капитала, како би се ојачала финансијска стабилност. Упркос предностима и позитивним ефектима, временом је показао неке недостатке, а за наше истраживање је кључно што преме датом стандарду адекватност капитала зависи од кредитног ризика, док су остали ризици (тржишни и оперативни) изостављени из анализе.[348]

Базел II се састоји из три стуба:[349]

1) стуб 1 дефинише минималне капиталне захтеве за кредитни, тржишни и оперативни ризик, уз могућност коришћења софистицираних модела и техника за њихово израчунавање;
2) стуб 2 учвршчује везу између оптималних капиталних захтева и врсте и степена ризика којима је банка изложена у свом пословању, уводећи процес интерне процене адекватности капитала (ICAAP) и јачајући процес супервизије;
3) стуб 3 употпуњује везу између стуба I и стуба II, истичући значај тржишне дисциплине увођењем минималних захтева за објављивање информација банака.

На основу Базел II НБС је донела следећа акта (објављена у „Службеном гласнику РС“, бр 45/2011 и 46/2011):[350]

- Одлука о адекватности капитала банке;
- Одлука о управљању ризицима банке;
- Одллука о објављивању података и информација банке;
- Одлука о контроли банкарске групе на консолидованој основи, и

[346] Огњановић, В., *op.cit.*
[347] Ibid
[348] Доступно на: https://www.nbs.rs/internet/latinica/55/55_2/55_2_2/index.html
[349] Доступно на: https://www.nbs.rs/internet/latinica/55/55_2/55_2_3/index.html
[350] Доступно на: https://www.nbs.rs/internet/latinica/55/55_2/55_2_3/o_propisima_bazel_II.pdf

– Одлука о извштавању и извештавању о адекватности капитала банке.

Базел III је донет на бази претходних споразума, као и на основу искустава светске финансијско-економске кризе. Измене се односе пре свега на тржишне ризике и секјуритизацију. Први пут су уведени минимални стандарди који се односе на захтеве у погледу ликвидности банака.[351]

Оперативни ризик је први ризик који инвестициона друштва морају оцењивати, знатно пре управљања кредитним и тржишним ризицима.[352]

Увођењем оперативног ризика у Базелски споразум II тежило се следећем:[353]

– постићи свеобухватнији трерман изложености ризицима, с обзиром да је први пут поред кредитних и тржишних ризика регулисан и оперативни ризик, као водећи ризик у групи нефинансијских ризика;
– дефинисању појма оперативног ризика;
– утврђивању међународно признатог оквира за израчунавање потребног капитала за укупне изложености ризицима, који обухватају и оперативне ризике;
– дефинисању оквира за истраживање и прикупљање података кроз понуђену класификацију оперативних ризичних догађаја у неколико категорија.

В. Матић наводи да је Базелски комитет за банкарски надзор објавио документ под називом „ Међународна мерења капитала и стандарди о капиталу, ревидирани оквир“, шире познат као Базел II, чиме се постигла нова архитектура базирана на три комплементарна концепта: минимуму капиталне адекватности, контролној функцији и тржишној дисциплини. Овај споразум захтева од банака да развијају робусне оквире за управљање ризицима, што даје следеће погодности:[354]

– обухватнији третман ризика (први пут се поред кредитног и тржишних ризика укључују оперативни ризици);
– шира лепеза понуђених приступа за мерење ризика и калкулација потребног капитала;
– софистицирани начин мерења ризика које омогућава прецизно одређивање ризичног профила банке и калкулацију потребног економског капитала;
– нов третман инструмената за ублажавање изложености ризицима

[351] Доступно на: https://www.nbs.rs/internet/latinica/55/55_2/bazel_3/index.html

[352] Совиљ, Р., Стојковић-Златановић, С.: *Модели управљања оперативним ризиком у инвестиционим друштвима у процесу европских интеграција Републике Србије*, Институт друштвених наука, Мегатренд ревија, Vol. 15, № 2, 2018: 1-16, 2018. година, доступно на: https://scindeks-clanci.ceon.rs/data/pdf/1820-3159/2018/1820-31591802001S.pdf

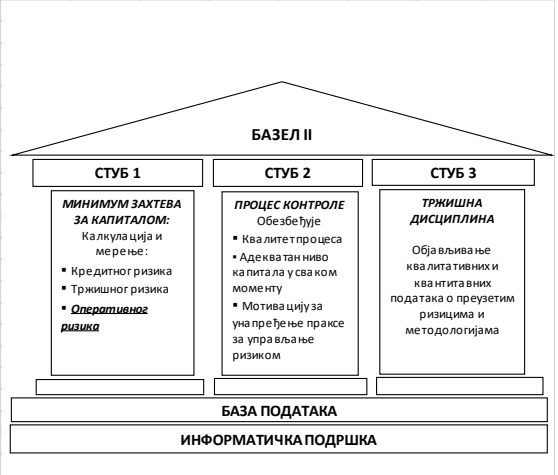
[353] *Ibid*

[354] В. Матић: *Базелски споразум II*, часопис Банкарство, број 7-8, 2009. година, доступно на: https://www.casopisbankarstvo.rs/Portals/0/Casopis/2009/7_8/B07-08-2009-Ekoleks.pdf

- у оквиру комплементаронг концепта („стуба“) контролне функције, дат је значајан нагласак широј улози националних контрола, и то не само у смислу развоја интерних метода за процену ризика, већ и у смислу да контролори процене ефекат који ризици производе у односу на различите методе утврђивања економског капитала;
- комплементарни концепт 3 („трећи стуб“), тржишна дисциплина, захтева од банака да јавно презентују висину капиталних трошкова, као и процедуре и механизме за контролу ризика.

Оперативни ризик, као нефинансијски ризик, представља ризик директних и индиректних губитака, који су последица неусаглашених поступака, као и људског, интерног и екстерног фактора, те уколико се приступи технолошком тумачењу поменуте дефиниције, примећује се синергија у деловању ризика људског фактора, ризика пословања, ризика трансакција, као и технолошких ризика.[355]

Схема број 17: ***Организација Базел II споразума***



Најзначајнији извори оперативног ризика су:

- интерне преваре – обухватају погрешно извештавање и друге неовлашћене активности попут непријављених или неовлашћених трансакција, крађе, корупције, фалсификовања, утаје пореза, намерног уништавања имовине, *злоупотребе личних података клијената,* инсајдерска трговања и друго;
- екстерне преваре – *обухватају физичке крађе, фалсификовање, неовлашћене упаде у информационе системе, крађу података* и друго;
- пропусти у односима са запосленима и у систему безбедности на раду – обухватају одговорност за запослене (безбедност и здравље на раду), обештећење запослених (исплата зарада, накнада, бенефиција, прекид радног односа и др.), као и све врсте дискриминације на радном месту;
- губици настали у односима са клијентима, пласманом производа или у пословној пракси – односе се на транспарентност пословања (као што су агресивна продаја,

[355] Совиљ, Р., Стојковић-Златановић, С., *op.cit.*, стр. 3. и 4.

нарушавање приватности, *злоупотреба поверљивих информација* и др.), неодговарајућу тржишну или пословну праксу (кршење антимонополских прописа, инсајдерско трговање, прање новца и др.), грешке у производима, лош избор клијената и друго;

- оштећење средстава и имовине – насталих услед природних катастрофа, вандалскихи или терористичких напада и друго;
- прикиди у пословању и пад система – односе се на *пад система проузрокован падом хардвера, софтвера, телекомуникацијских проблема, прекидом у напајању електричном енергијом, гасом, водом и друго*;
- губици настали извршењем трансакција, испоруком и процесима управљања – односе се на евидентирање и извршавање трансакција (на пример: *погрешан унос података*, неоперативност, пропуштени рокови, рачуноводствене грешке, погрешне испоруке и др.), пропусти у обавезном извештавању, непотпуна документација клијента, *неовлашћени приступ рачунима клијената*, штета на имовини клијената, различите врсте спорова и друго.

Овако широка категорија оперативних ризика, где смо напоменули да ово није коначна листа могућих догађаја који представљају оперативни ризик, могуће је да се сведе на три категорије, применом критеријума учесталости реализације, као и могућих последица, према следећем:[356]

- стандардни оперативни ризици: прате редовне, текуће активности у пословању и у просеку се догађају једном недељно, а губици су мале вредности;
- кључни оперативни ризици: јављају се ређе, али проузрокују веће губитке наспрам стандардних, али не могу својим износом да угрозе опстанак организације;
- изузетни оперативни ризици: катастрофални, или „ризици убице“, јављају се изузетно ретко (једном у десет година), али су последице толико разорне, да онемогућавају реализовање стратешких циљева друштва, а понекад прете и њиховом опстанку.

Банке и финансијске институције су обавезни да рачунају економски капитал за неочекиване губитке који настају реализацијом оперативних ризика (увођење „стуба“ капиталних захтева који је директно везан за оперативне ризике), али и да праве планове пословања у ванредним околностима.

Оперативни ризици су у порасту у банкарској индустрији, услед следећих утицаја:

- пораста електронске трговине;
- пораста аквизиција и мерџера у банкарском сектору;[357]

[356] *Ibid,* стр. 4. и 5.

[357] „Јак замах мерџера и аквизиција банкарских институција у развијеним земљама Европске уније је саставни део глобалних процеса прекомпозиције и укрупњавања банака, али и резултат стварања јединственог финансијског тржишта које је подстакнуто увођењем евра као јединствене валуте“. С. Машић: *Мерџери и аквизиције у европском банкарству*, докторски рад, Универзитет Сингидунум, Београд, 2009. година, стр. 12.

- употребе технологија са високом аутоматизацијом, што доводи до преноса ризика грешака које настају на основу ручне обраде, ка ризицима отказивања система, што има велики негативан исход догађаја;
- пораст броја и врста услуга на тржишту које пружају банке и финансијске институције;
- пораст тренда *outsourcing*-а појединих услуга у банкарству.

Приступ управљању оперативним ризицима зависи од више фактора (величина организације, кадровска и техничка опремљеност, обим и сложеност послова и др.), али упркос тим бројним разликама базелски комитет и директиве ЕУ препознали су да је главни оквир за ефикасно управљање оперативним ризицима: дефинисане стратегије, надзор одбора директора, систем унутрашње контроле (хијерархија и подела надлежности), извештавања, као и планирање у случају непредвиђених догађаја.[358]

Следствено томе, видели смо у анализи *Одлуке у управљању ризика у банкама*[359], да је су надлежности у банкама организоване према следећем:

- Одбор директора – усваја стратегије управљања оперативним ризицима. Кључни део је одобравање толерисаног ризика од сране организације. Одговоран је за ефикасан надзор над процесом управљања оперативним ризиком, за разматрање политика и процедура, преиспиривање планова за ванредне ситуације. Усваја план континутитеа пословања (BCP) и план опоравка активности у случају катастрофа (DRP)
- Запослени задужени за управљање оперативним ризицима – прате изложеност оперативном ризику према врстама, узроцима и значају догађаја и о томе редовно извештавају чланове управе

Од посебне важности за наш предмет истраживања, јесте истицање *значаја подизања свести запослених и културе понашања* у односу на изложеност оперативним ризицима, од стране Базелског комитета, као једног од приоритета у управљању оперативним ризицима.

Постигнути успех у управљању ризицима директно зависи од начина на који се разуме и осећа процес управљања, јер су оперативни ризици уједно и ризици културе професионалног понашања свих запослених. Степен развијености културе понашања наспрам изложености оперативним ризицима, манифестује се као мања или већа осетљивост запослених на ове ризике, што прати и одговарајући степен могућих губитака. Чести су случајеви да се запослени суочавају са оперативним ризицима, а да тога нису ни свесни.[360]

[358] Совиљ, Р., Стојковић-Златановић, С., *op.cit.*, стр. 6.
[359] „Службени гласник РС, бр. 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 – др. одлука 1, 43/2013, 92/2013, 33/2015, 61/2015, 61/2016, 103/2016 и 119/2017
[360] Совиљ, Р., Стојковић-Златановић, С., *op.cit.*, стр. 7.

Методи за мерење и управљање оперативним ризицима промовисани су Базелом II (2004. године), а уведене су у европско законодавство 2013. године, усвајањем Директиве о адекватности капитала и Уредбе о капиталним зхтевима.[361]

У овим документима реч је о три основна метода за мерење оперативних ризика:

- приступ основног индикатора (енгл: *basic indicator approach – BIA*);
- стандардизовани приступ (енгл: *standardized approach – SA*);
- приступ напредног мерења (енгл: *advanced measurement approach – AMA*).

Приступ основног индикатора (БИА), је најједноставнији метод израчунавања минимума нужног капитала и уједно најмање прецизна (одакле се не препоручује за велике интернационалне банке). Трогодишњи просек нето оперативног прихода банке множи се са фикскним алфа постотком (15%).[362]

Стандардизовани приступ (СА), капитални захтев за кредитни ризик израчунава се тако да се укупне активности банке поделе на осам пословних линија (корпоративне финансије, трговање и продаја, пословање са становништвом, комерцијално банкарство, плаћање и наплата, агенцијске услуге, управљање имонивом, малопродајна брокерска делатност), потом се нето оперативни приход сваке пословне линије множи са бета фактором прописаним за сваку послвону линију. Укупни минимум нужног капитала израчунава се као збир појединачних минимума за осам пословних линија.

Да би банка могла да примени стандардизовни приступ, Базел II је прописао минималне квалитетне захтеве који требају да су испуњени:

1) банка мора да формира организациону јединицу која ће имати јасну слику одговорности за управљање оперативним ризиком;
2) банка мора да осигура редовно праћење података о оперативном ризику, укључујући значајне губитке по појединој пословној линији;
3) виши извршни менаџмент банке, управа и надзорни одбор требало би да добијају редовне извештаје о изложености оперативном ризику;
4) систем управљања оперативним ризиком треба да буде добро документован (интерне политике, контроле и процедуре везане уз систем управљања оперативним ризиком);
5) систем управљања треба редовно подвргавати независним проверама.

[361] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, O. J. L 176/2013 (Директива о адекватности капитала) и − Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) 648/2012 O. J. L 176/2013 (Уредба о капиталним захтевима).

[362] Вуковић, В.: *Ризици у банкарству са посебним освртом на оперативни ризик*, магистарски рад, Сингидунум, Београд, 2009. година, стр. 22. – 23. Доступно на: https://singipedia.singidunum.ac.rs/izdanje/42127-rizici-u-bankarstvu-sa-posebnim-osvrtom-na-operativni-rizik

Приступ напредног мерења (AMA), дефинише се тако да за прорачун минималног нужног капитала се користе банкарски интерни системи за управљање оперативним ризиком под условом да су задовољени квантитативни и квалитативни захтеви наведени у стандарду. За коришћење АМА приступа банка мора да добије сагласност супервизора.

Квалитативни захтеви су идентични онима које банка мора да испуни да би примењивала стандардизовани приступ.

Код квантитативих захтева се не воде специфични параметри, јер управљање ризиком континуирано еволуира. Банка мора да докаже да је својим моделом убухватила и оне (малобројне) губитке са катастрофалним последицама. Овде се подразумева и редовно прикупљање интерних података о губицима и коришћење екстерних података у одређеним случајевима; ангажовање стручњака који ће спроводити анализу. У обзир се узимају и кључне карактеристике окружења и чинилаца интерне контроле који могу изменити свој профил оперативног ризика, те коришћење техника за смањивање изложености оперативном ризику.

Прва два метода су регулисана у европском законодавству, а приступ напредног планирања даје много више креативне слободе (могућност развијања сопствених метода).

Ови приступи, како наводе Р. Совиљ и С. Стојковић-Златановић, позивајући се на *Одлуку о адекватности капитала банке* (Службени гласник РС, бр. 46/2011, 6/2013 и 51/2014, Члан 405), уведени су за банке у домаћи правни систем. Овлашћена банка може изабрати један од понуђених (три) приступа, уз претходну сагласност НБС. Изузетно, банци је дозвољено да комбинује приступе за рачунање капиталног захтева за оперативни ризик.[363]

У домаћем праву водило се рачуна о избегавању двоструког израчунавања капиталних захтева када су у питању овлашћене банке. Тако се *интерни подаци о губицима који су настали по основу оперативног ризика*, а повезани су са кредитним ризиком и укључени у интерну базу историјских података о кредитном ризику, *евидентирају у интерној бази података о оперативном ризику и посебно се означавају*. Уколико је банка те губитке обухватила при рачунању капиталног захтева за кредитни ризик, не узима их у обзир при рачунању оперативног ризика. Исто тако, банка је обавезна да губитке који су настали по основу оперативног ризика, а повезани су са тржишним ризицима, укључи у израчунавање капиталног захтева за оперативни ризик, а не у тржишне ризике.[364]

В. Ковачевић, наводи да је већина банака кроз своју пословну политику утврдила да се за процењивање оперативног ризика користи *RCSA* који је усмерен на утврђивање профила оперативног ризика.[365]

---

[363] Совиљ, Р., Стојковић-Златановић, С., *op.cit.,* стр. 8.
[364] *Ibid,* стр. 11.
[365] Ковачевић, В.: *Модели управљањеа ризиком у банкарскмо сектору*, докторска дисертација, Факултет за економију и превредни менаџмет, Универзитет привредна академија, Нови Сад, 2016. година, стр. 198. – 202., доступно на: http://nardus.mpn.gov.rs/bitstream/handle/123456789/6690/Disertacija4785.pdf?sequence=1&isAllowed=y

RCSA је акроним од енгеског појма *Risk Control Self Assessment,* што означава процес у којем менаџмент и запослени на свим нивоима идентификују и процењују ризике и повезане контроле.[366]

Методологија се стриктно и доследно спроводи на нивоу целе банке и њен је циљ да се:

- идентификују оперативни ризици;
- процене оперативни ризици и њихово окружење;
- утврди профил оперативног ризика и његова изложеност путем квантитативног приступа.

Процес идентификације ризика треба да укључи радионице где ће се окупити власници ризика, са циљем да се обезбеди потпуно разумевање проблема и угрожености у погледу постизања пословних циљева и помогне усмеравање на идентификацију ризика ка кључним ризицима. Циљ радионице јесте да се идентификују ризици који су уско повезани са сваким процесом рада који обавља јединица/одељење и да се тачно формулишу и дефинишу. Јачина оперативног ризика ближе се одређује као комбинација вероватноће и утицаја. Пракса банака познаје најмање три нивоа јачине ризика, и то:[367]

- велика јачина, власник ризика прави и предлаже акциони план за предузимање мера и доставља га надлежним органима на одобрење. Власник ризика успоставља контролу и идентификује кључне показатење ризика и даље их, са аспекта изложености банке ризику, контролише;
- средње јачине, уз опреност и дискрецију, власник ризика доставља акциони план и доставља га надлежним органима на одобрење. Власник ризика може да успостави и кључне показатеље ризика у ниво најозбиљнијих ризика ко ће се десити у блиској будућности;
- мале јачине, код оваквих оперативних ризика неће се осмишљавати ни један акциони план нити ће се истицати кључни показатељи ризика.

Како смо претходно навели у овом поглављу, Базел III је надоградио споразуме Базел I и Базел II, али је за наш предмет истраживања од значаја споразум Базел II, због чега смо му посветили потребну пажњу.

Извршни одбор НБС усвојио је следеће прописе објављене у „Службеном гласнику РС“, број 103/2016, којима су уведени Базел III стандарди у Републици Србији:[368]

- Одлука о адекватности капитала банке;
- Одлука о објављивању података и информација банке;
- Одлука о извештавању о адекватности капитала банке;
- Одлука о изменама и допуне Одлуке о извештавању банака;

[366] Доступно на: https://financetrainingcourse.com/education/2015/04/rcsa-risk-control-self-assessment/
[367] Ковачевић, В., *op.cit*
[368] Доступно на: https://www.nbs.rs/internet/latinica/55/55_2/index.html

- Одлука о управљању ризиком ликвидности банке;
- Одлука о изменама и допунама Одлуке о ушправљању ризицима банке.

Поред усклађивања, с релевантним правним актима ЕУ у области банкарства, основни циљеви усвајања ових прописа су повећање отпорности банкарског сектора повећањем квалитета капитала и увођењем заштитних слојева капитала, боље праћење и контрола изложености банке ризику ликвидности, даље јачање тржишне дисциплине и транспарентност пословања банака у Републици Србији објављивањем свих релевантних информација о пословању банке, као и прилагођавање извештајног система новим регулаторним решењима.

5.2. Резилијентност информационих система у банкама и финансијским институцијама

У досадашњем истраживању закључили смо да у свету глобалног финансијског система постоје одређене међузависности које су изазване следећим факторима:

- развој информационих система, а посебно дигитализације, довео је до промена у пословању, тако што се многи пословни процеси преносе у дигиталну сферу, што последично доводи до новог начина њиховог обављања, као и до нових услуга, које су посебно изражене у банкарству;
- информације су постале стратешки ресурс, одакле се њиховој заштити посвећује све већа пажња;
- извори претњи за неповредивост информација се шире, а начини угрожавања постају једанко софистицирани као што су и нови начини пословања које доноси технолошки напредак;
- савремено друштво све више улаже у механизме заштите информација, а те мере нису само техничке природе, већ и организационе, нормативне и друге природе;
- банкарски систем је део глобалног финансијског система, и не може се поматрати само на националном нивоу. У ту сврху постоје бројне међународне организације, које доносе нормативне оквире и стандарде чија је сврха и заштита информација у најширем контексту, а у које се уклапају регулатори на националним нивоима, који на овој основи праве локалне нормативне оквире у које се опет уклапају друштва која им припадају;
- област банкарства, прати трендове који утичу на амбијент пословања овог сектора, и у том смислу највише су у употреби Базел споразуми који су утицали на локалне регулаторе, у нашем случају НБС, да у оквиру своје надлежности донесу тематске нормативне, организационе и контролне мере;
- област заштите информација претежно припада категорији оперативних ризика, а односи се и на друге ризике у банкарству, у мери у којој и саме информационе технологије утичу на пословање;

– Базел II споразуми уврстили су оперативне ризике у најважније ризике којима је изложена банкарска индустрија.

Поред до сада предузетих мера, и свесни недоследности које се односе на терминолошку (и практичну) неусклађеност у остваривању заштите информација, где се због свог неупитног значаја информационих технологија, целокупна област заштите информација претежно бави феноменом информационе безбедности, у циљу даљег изучавања нашег предмета истраживања желимо да сагледамо простор који отвара нове перспективе у остваривању заштите информација у банкама и финансијским институцијама.

Традиционална процена ризика подразумева сагледавање проблемске области кроз односе претњи, рањивости и последица које ће наступити, и у том смислу кибернетска безбедност постаје ограничена јер су потребни приступи за решавање претњи и рањивости који су примењиви (и ефиксни) у околностима сложених и међусобно повезаних система, одакле је тешко извести процену ризика која ће предвидети каскадне ефекте који би се могли догодити.[369]

Непредвидивост, екстремна несигурност и брзи развој потенцијала сајбер претње стварају ситуацију у којој је процена ризика све више неспособна да пружи адекватне одговоре који се односе на сајбер безбедност великих система, а посебно критичних инфрастуктура. Једина одговарајућа одбрана, наводе Линков и Кот, била би одвајање сајбер система од интернета, на исти начин на који биолошки системи развијају имунитет од инфекција и других напада, одакле се и сајбер системи морају прилагодити на сличан начин.[370]

Из ових разлога, *cyber resilience*, односи се на способност система да се припрема, апсорбује, прилагођава и опоравља од штетних ефеката сајбер напада.

У току нашег истраживања нисмо пронашли одговарајући појам за резилијентност (енгл: *resilience*), а најближи термин објашњењу овог појма би био термин *отпорност*, који не одражава у потпуности његово значење (али је најприближнији).

Најприближнија објашњења резилијентости пронашли смо у области психолошких наука.

Resiliance је способност да поново будете срећни, успешни итд., након што се десило нешто тешко или лоше.[371]

За разлику од психотерапије која има за циљ лечење психичких поремећаја психолошким путем, програм за развој резилијентности се бави јачањем природног потенцијала сваког

[369] Linkov, I., Kott, A.: *Cyber Resilience of Systems and Networks*, preprint version, Springer 2018., доступно на: https://www.researchgate.net/publication/325680212_Fundamental_Concepts_of_Cyber_Resilience_Introduction_and_Overview
[370] *Ibid*

[371] Доступно на: https://dictionary.cambridge.org/dictionary/english/resilience

човека за развој и раст и на тај начин служи као превенција настанка психолошких сметњи и поремећаја.[372]

Термин резилијентност усвојен је из енглеског језика, зато што је тешко наћи једну реч у српском језику која би пренела вишеслојно значење појма *resilience*. У енглеском овај појам се користи када се говори о отпорности на спољашне услове, прилагодљивости променама, превазилажењу животних недаћа. За коров се каже да је резилијентан – чупамо га, заливамо хемикалијама, а он наставља да расте упркос свему томе.[373]

Резилијентност је динамички процес позитивне адаптације у контексту значајне недаће. Постоје различите дефиниције резилијентности као и теорије, али је заједничко свима да препознају два услова да би о њој могли да говоримо: изложеност претњи или озбиљној недаћи и – постизање позитивне адаптације упркос великим нападима на развојни процес.[374]

Cyber Resilience, је предвиђање и прилагођавање променама у окружењу, задржавање и брзи опоравак од сајбер инцидента, наводи Сајбер лексикону који је издао Одбор за финансијску стабилност (енгл: *Financial Stability Board – FSB*).[375]

Линков и Кот наводе да је резилијентност својствена за социо-екологију, психологију, организације и инжењеринг и дају преглед садржаја активности резилијентности по временским фазама које обухватају: планирање, апсорбовање, опоравак и прилагођавање, где наводе особине/разлике за сваку од њих појединачно (Табела број 9: *Преглед резилијентности различитих система*).

Планирање подразумева одређивање критичних функција (услуга), апсорбовање препознавање прагова (граница) након којих је догађај инцидент (или унутрашња толеранција на стрес), опоравак и прилагођавање подразумевају дефинисање потребног времена за ове активности (трајање смањених перформанси система), а прилагођавање − промену приступа или учење из претходног догађаја.[376]

Слично другим областима, како је наведено у претходном табеларном прегледу, сајбер резилијентност се односи на способност система да се опоравља после сајбер напада. Напад производи деградацију перформанси, а што се систем опорави на виши ниво перформанси, то има већу резилијентност (Графикон број 11: *Приказ тока сајбер резилијентности*).

---

[372] Доступно на: http://rezilijentnost.blogspot.com/p/o-programu.html

[373] Доступно на: https://www.lovesensa.rs/print/clanci/srecan-zivot/otporni-na-nevolje

[374] Желесков Ђорић, Ј.: *Резилијентност и задовољство послом хирурга*, Институт за криминолошка и социолошка истраживања, Београд, 2012. година, стр. 31.

[375] ФСБ је тело које су основали шефови фржава и влада Г 20, у циљу промоције реформе међународне финансијске регулације и надзора. Доступно на: https://www.fsb.org/2018/07/cyber-lexicon-consultative-document/

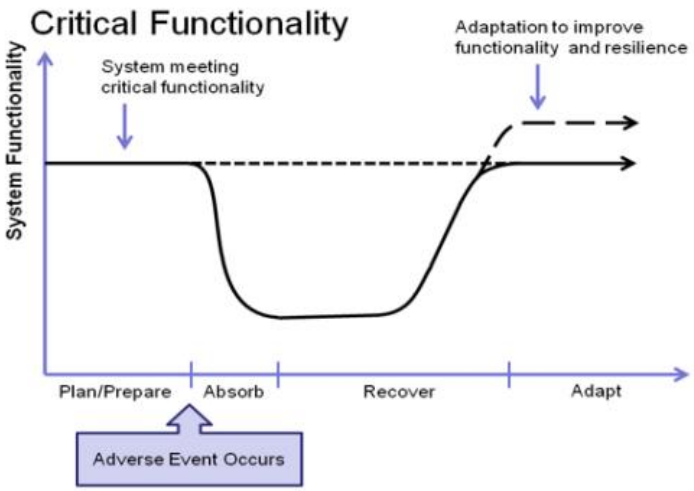
[376] Linkov, I., Kott, A I., op. cit., стр. 6

Традиционалну процену ризика карактерише квантитативни метод, услед чега се лакше одређује прагови ризика, које је онда потребно формализовати у документима. Карактеристика оваквог приступа је укључивање вероватноће наступања догађаја и последица коју она производи за систем.

Табела број 9: ***Преглед резилијентности различитих система***

Фаза резилијентности	**Карактеристике отпорности**	**Област**			
		Социо-еколошки	Психиолошки	Организациони	Инжењеринг& Инфраструктура
Планирање	Критичне функције	**Функција система која је важна за мерење перформансе**			
		Екосистем битан за заједницу	Психолошко стање	Пружањење роба и услуга	Функционалност система
Абсорбовање	Прагови	**Унутрашња толеранција на стрес**			
		Природни услови амбијента	Карактеристике личности и очекивања окружења	Организацини капацитети	Осетљивост функционалности
Опоравак	Време	**Тајање смањених перформанси система**			
		Промене током времена	Зависи од доба живота (младост или одрасла особа)	Потребно време опоравка	Потребно време опоравка
Адаптација	Сећање/ адаптибивни менаџмент	**Промене у приступу на основу искуственог учења**			
		Искуство система како да се опстаје	Психолошка еластичност или стрес	Организационе промене за будуће изазове	Редизајн система базиран на искуствима и спреман за будуће изазове

Графикон број 11: ***Приказ тока сајбер резилијентности***[377]



Сајбер стварност међутим карактеришу нове претње са несигурним интензитетом, као и тешко предвидљивом одређивању учесталости и рањивости. Одређивање хипотетичких претњи, или сценарија, води до великог скупа догађаја и последица који могу заузети вредности од оних са малим утицајем, до последица које су катастрофалне за систем, што значи да су и недоступне за апсорбовање, опоравак и адаптацију система.

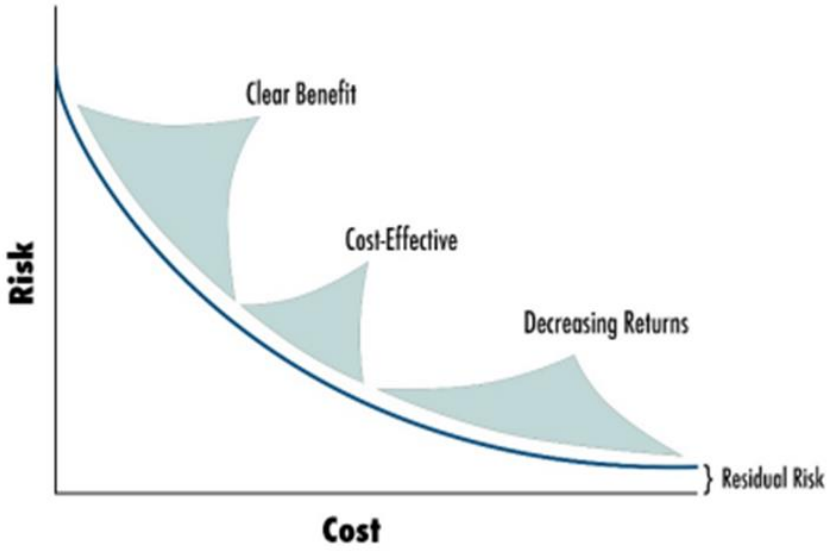
Кључна стратегија управљања ризиком, како наводе Линков и Кот, је идентификација критичних процеса, а затим њихово очвршћавање.

Овакав приступ је прикладан за изоловане информационе системе, али када претње практично нису познате, тешко је идентификовати све критичне компоненте и постаје скупо поступити конзервативно и улагати у ојачавање свих делова система и још то урадити од свих врста могућих претњи (Графикон број 12: *Однос нивоа ризика и цене улагања у превенцију штета*).

Последица традиционалног приступа је, како видимо на дијаграму, да цена улагања стално расте, уколико је амбиција да се заштите сви делови система и од свих претњи. То доводи да тражења стално нових извора финансирања, односно до стагнације на том плану. За то време, информациона инфраструктура остаје у великој мери неспремна за инцидентне догађаје.

[377] *Ibid*, стр. 8

Графикон број 12: ***Однос нивоа ризика и цене улагања у превенцију штета***[378]



Не мања важна чињеница је да је у савременом пословном свету све мање изолованих информационих система, већ су сви они међузависни и повезани, што практично чини немогућим квантификацију ризика.

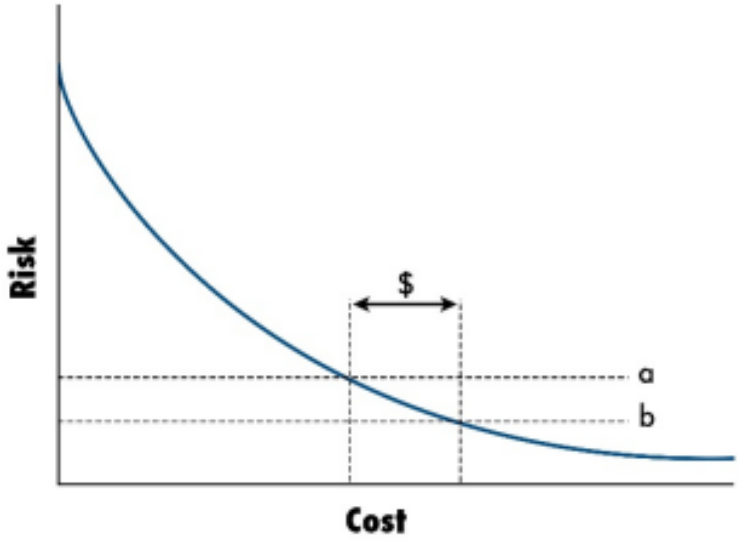
Уместо потребе да се захтева већа превенција, финансирање се може преусмерити на напоре за јачање резилијентности. Системи који су већ формирали ефективну превенцију могу средства да преусмере ка резилијентности прихватањем тренутног нивоа ризика.

Линков и Кот дају дијаграм на којем је додатно објашњена идеја да се буџет који би се потрошио на већу превенцију усмери ка ризилијентности, уместо да се (нефункционално, јер ће се увек јављати нове претње, у околностима када је информациони систем повезан са другим таквим системима и тај скуп се непрекидно шири) улаже у даљу превенцију (Графикон број 13: *Прихватање постојећег нивоа (ефективног) ризика а) и трошење буџета за резилијентност уместо постизања хипотетички мањег нивоа ризика б*.)

На примеру овог дијаграма, идеја резилијентности је да се прихвати ниво ризика означен са а), а да се буџет који би се потрошио за превенцију која би довела до нивоа означеног са б) уложи у резилијентност. Том приликом остаје задатак одређивања нивоа ефективног ризика, где се тек очекује допринос науке и струке.

[378] *Ibid,* стр. 10

Графикон број 13: ***Прихватање постојећег нивоа (ефективног) ризика а) и трошење буџета за резилијентност уместо постизања хипотетички мањег нивоа ризика б)***[379]



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

Банка за међународна поравнања (енгл: *Bank for International Settlements – BIS*) има мисију да служи централним банкама у њиховоом остваривању монетарне и финансијске стабилности, подстиче међународну сарадњу у тим областима и делује као банка за централне банке. Основан је 1930 године и данас је у власништву 62 централне банке које представаљајуј земље из целог света, које заједно чине 95% свеског БДП-а, са седишем у Базелу и има своја представништва у Хонг Конгу и у Мексико Ситију.[380] Претходно смо изнели да је Народна банка Краљевине Југославије је била чланица од 1931. године. Учешће СФРЈ је замрзнуто 1992. године, а СР Југославија је 2001. године обновила чланство. НБС је 2009. године је наставила чланство са 2.920 акција. У мају 2012. године НБС је постала члан Мреже за унапређење управљања централним банкама у оквиру БИС-а.

Међународна организација комисија за хартије од вредности (енгл: *International Organization of Securities Commissions − IOSCO*), је међународно тело које окупља светске регулаторе хартија од вредности и у том смислу је признато као тело које поставља светске стандарде за сектор хартија од вредности. ИОСЦО развија, имплементира и промовише придржавање међународно признате стандарде за регулисање хартија од вредности.

[379] *Ibid*, стр. 11
[380] Доступно на: https://www.bis.org/about/index.htm?m=1%7C1

Интензивно сарађује са Г20 и Одбором за финансијску стабилност (ФСБ) на плану глобалне регулаторне форме.[381]

Група 20 (или Г20) представља међународни форум влада и гувернера централних банака из 19 земаља и Европске уније. Основана је 1999. године са циљем промовисања међународне финансијске стабилности. Од 2008. године Г20 је проширила свој дневни ред, где шефови влада и председници држава, као и министри финансија и министри спољних послова повремено учествују на самитима ове организације. Настоји да се бави питањима финансијске стабилности која превазилазе одговорности било које организације. ЕУ представља *Европска комисија* и *Европска централна банка*. Економије Г20 заједно чине око 90% бруто светског производа, 80% светске трговине, две трећине светске популације и својом организацијом покрива око половине светске површине.

Народна банка Србије има сарадњу са Европском централном банком од 2008. године, кроз реализацију различити пројеката, и то:[382]

- пројекат техничке помоћи Европске централне банке НБС под називом „Анализа потреба Народне банке Србије“, а у оквиру пројекта у којем је учествовало 17 националних централних банака Европског система централних банака. Резултат пројекта је Извештај о анализи потреба НБС, с препоруком за унапређење пословања у областима у којмиоа је потребно извршити одређена усклађивања ради оперативних припрема НБС за укључивање у Европски систем централних банака;
- пројекат „Јачање институционалних капацитета НБС“, са учешћем експерата из 21 централне банке земаља ЕУ, а који је обухватио 13 области пословања НБС (између којих су и усклађивање законодавства и информациона технологија), у којима су усвојене стратегије, интерне смернице и економски модели, чија примена треба да омогући усаглашавање пословања НБС са стандардима централних банака Европског система централних банака, као и припрему закона у који је укључен регулаторни оквир ЕУ. Пројекат је трајао од 2011. до 2013. године;
- споразум о сарадњи у области спречавања прања новца о откривања фалсификованих новчаница евра у РС, из 2014. године, који представља први споразум између Европске централне банке и НБС;
- унапређење законодавног оквира НБС у сарадњи са ЕУ одвија се кроз два пројекта која се воде у сарадњи са Немачком агенцијом за међународну сарадњу, као и кроз пројекте *Plac II* и *Plac III* (енгл: *Policy and Legal Advice Centre*);
- током 2018. године, почела је реализација *IPA* пројекта „Јачање институционалних капацитета НБС у процесу приступања ЕУ”, у десет области пословања, између којих је су и информационе технологије. Циљ пројекта је наставак јачања институционалних и административних капацитета НБС усклађивањем њених функција и активности с прописима ЕУ и међународним стандардима. Спроводи се у сарадњи са *Twinning* партнерима – Бундесбанком, Народном банком Румуније,

[381] Доступно на: https://www.iosco.org/about/?subsection=about_iosco
[382] Доступно на: https://www.nbs.rs/internet/latinica/40/40_2/index.html

Хрватском народном банком, Хрватском агенцијом за надзор финансијских услуга и Немачком агенцијом за међународну сарадњу;

– Централна банка Немачке и Европска комисија покренуле су у марту месецу 2019. године, двогодишњи регионални пројекат „Програм за јачање капацитета централних банака Западног Балкана у оквиру интеграција у Европски систем централних банака", чији су крајњи корисници централне банке и банкарска супервизорска тела кандидата и потенцијалних кандидата за приступање ЕУ.

Одбор за финансијску стабилност (енгл: *Financial Stability Board – FSB*) је међународно тело које надледа и даје препоруке у вези са глобалним финансијским системом. Промовише међународну финансијску стабилност координирајући национална финансијска тела и међународна тела за утврђивање стандарда. Развијају регулаторне, надзорне и друге политике финансијског сектора. ФСБ настоји да ојача финансијске системе својих чланица и на тај начин допринесе стабилност међународног финансијског тржишта. Политике које развија спроводе национални органи. Основне функционалности су:[383]

– да процени рањивости које утичу на гобални финансијски систем, као и да се утврде регулаторне, надзорне и повезане радње потребне за њихово решавање;
– да промовише и координира размену информација између органа одговорних за финансијску стабилност;
– да надгледа и саветује о развоју тржишта и последицама на регулаторну политику;
– да координира рад међународних тела за утврђивање стандарда и развоја политика, како би се осигурала правовременост, координисаност и приоритизација у решавању утврђених недостатака;
– да прати и саветује најбољу праксу у испуњавању регулаторних стандарда;
– да подржава планирање у ванредним ситуацијама за прекогранично управљање кризама, посебно у погледу системски важних привредних система;
– да сарађује са Међународним монетарним фондом (ММФ) на спровођењу вежби раног упозоравања;
– да промовише примену договорених обавеза, стандарда и препорука политика кроз праћење примене од стране надлежних тела држава чланица.

Банка за међународна поравнања (БИС), преко Одбора за плаћања и тржишну инфраструктуру (енгл: *Committee on Payments and Market Infrastuctures*) и *Међународна комисија за хартије од вредности* (ИОСЦО), донели су Водич за сајбер отпорност финансијске тржишне инфраструктуре.

Полазећи од предмета истраживања, овом документу ћемо у даљим разматрањима посветити потребну пажњу.

[383] Доступно на: https://www.fsb.org/about/

5.4. Водич за сајбер резилијентност финансијске тржишне инфраструктуре

Како смо претходно изнели, овај документ је настао у сарадњи Банке за међународнано поравнања (БИС) и Међународне комисије за хартије од вредности (ИОСЦО).[384]

Инфраструктура финансијских тржишта (енгл: *Financial market infrastuctures – FMIs*) је кључна за одржавање и промовисање финансијске стабилности и економског раста. Доношење овог документа (водича, упутства, смерница) има за циљ да допринесе међународној активности у напорима финансијске индустирије да повећа своју сајбер резилијентност. То укључује способност финансијског тржишта да спречи сајбер нападе, брзо и ефикасно реагује на њих и постигне брже и сигурније циљеве опоравка. Поред тога, Водич за сајбер резилијентност, као међународно договорене смернице, пружа регулаторима подршку доследном и ефикасном надзору инфраструктуре финансијског тржишта у области сајбер ризика.

Суштински, намера приликом доношења овог акта била је развој културе свести о сајбер ризику, који води ка континуираним активностима поновљених процена и побољшања ставова о сајбер резилијентности на свим нивоима организације. Издавач документа је на овај начин желео да допринесе стандардима инфраструктуре финансијског тржишта, поред оних који су наведени у докумемту *Принципи за инфраструктуру финансијског тржишта* (енгл: *Principles for Financial Market Infrastructures – PFMI*).[385]

Овај документ се ослања на *Принципе за инфраструктуру финансијског тржишта* – ПФМИ принципе, други документ, који је настао 2012. године и донет је од стране Одбора за платни систем и поравнање (енгл: *Committee on Payment and Settlement Systems – CPSS*, а сада са називом *CPMI*) и Техничког комитета Међународне организације комисија за хартије од вредности (ИОСЦО).[386]

Документ је део скупа од 12 кључних стандарда које међународна заједница сматра кључним за јачање и очување финансијске стабилности. Он предвиђа 24 начела која се морају поштовати, у вези са управљањем тржишним ризиком у инфраструктури финансијских тржишта. Банка Енглеске захтева од својих оператера да се придржавају ових принципа.[387]

За наш предмет истраживања од значаја је да Принципи (ПФМИ) *препознају оперативни ризик, у које је укључен кибернетички ризик*, као посебан кључни ризик.

У уводном делу Водича наводе се неке карактеристике сајбер ризика, и контатује се да иако су део оперативних ризика, да због своје специфичности представљају изазове за

[384] *Guidance on cyber resilience for financial market infrastructures*, Bank for International Settlements and International Organization of Securities Commissions, 2016. године, доступно на: https://www.bis.org/cpmi/publ/d146.htm
[385] *Ibid*
[386] *Principles for Financial Market Infrastructures (PFMI),* доступно на: https://www.bis.org/cpmi/info_pfmi.htm
[387] *Ibid*

традиционално управљање ризицима (што смо и ми навели у дефинисању појма резилијантности сајбер система), према следећем:

i. одлика сајбер напада је софистицираност и упорна природа. За разлику од других извора ризика, ове нападе је обично трешко препознати;
ii. постоји широк спектар улазних тачака кроз који финансијске институције могу бити угрожене. То је последица међусобне повезаности свих учесника који се јављају у инфраструктури финансијског тржишта. Овде се дакле не мисли само на финансијске институције, већ и на све оне организације које на било који начин учествују у остваривању пословних функција, а повезани су преко информатичке мреже са финансијском институцијом. Још једна важна карактеристика је да се напад може догодити и на наизглед не тако важном ентитету у систему, чија је можда највећи значај, у смислу ове дискусије, то што представља ентитет система (омогућава улазак, на пример злонамерном софтверу). Сајбер ризик није дакле нужно повезан са степеном важности неког ентитета у систему. Из сајбер перспективе, добављач некритичких услуга, или малог обима, или мале вредности добављених услуга, може бити једнако ризичак као и критични (по дефиницији) добављач услуга. Овде припада и инсајдерска претња, и у овом смислу је готово свеједно да ли је реч о злонамерном или непажљивом запосленом;
iii. одређени сајбер напади могу да се одиграју управо преко делова система који су дизајнирани за управљање ризицима и чија је сврха континуитет пословања. У случају безбедносног инцидента, на пример, када је потребно хитно ископирати податке, управо ова радња може допринети ширење злонамерног софтвера.
iv. Сајбер напади могу да буду невидљиви и да се брзо шире у мрежама. Они се управо тако и дизајнирају, да могу да прођу неопажено контроле, одакле финансијске инфраструктуре захтевају брзо откривање, реаговање, задржавање и опоравак од оваквих напада.

Водич за сајбер резилијентност, већ је напоменуто, наслања се на Принципе за инфраструктуру финансијског тржишта, и у том смислу потенцира следеће принципе:

- начело 2: *Управљање* – инфраструктура финансијских тржишта (ФМИ) треба да има тако организовано управљање да је оно јасно и транспарентно;
- начело 3: *Оквир за свеобухватно управљање ризицима* – ФМИ треба да има оквир за управљање правним, кредитним, ликвидним, оперативним и другим ризицима;
- начело 8: *Коначност нагодбе* – односи се на период када је потребно завршити финансијске трансакције које обављају ФМИ, за које ово начело каже да треба да буде у реалном времену или у оквиру једног радног дана;
- начело 17: *Оперативни ризик* – ФМИ треба да идентификује веродостојне изворе оперативног ризика (спољашње и унутрашње) и да ублажи њихов утицај употребом одговарајућих система, политика, процедура и контрола. Системи треба да буду тако дизајнирани да обезбеде висок степен сигурности и радне поузданости. Управљање континуитетом пословања треба да има за циљ правовремени опоравак пословања и

испуњавање активности финансијске институције, укључујући и случајеве великог поремећаја;
- начело 20: ФМИ повезаност – ако је инфрастуктура финансијског тржишта (ФМИ) повезана са другом таков инфраструктуром, тада она треба да надледа и управља ризиком који се односи на тај однос.

Водич наглашава потребу коначности поравнања у трансакцијама и потребу завршетка критичних операција. У том смислу два су важна елемента:

- важност измирења приликом доспевања обавеза за финансијску институцију и коначност тих трансакција;
- способност финансијске институције да настави рад у року од два сата након поремећаја.

Водичу одређује пет категорија на које треба одговорити путем сајбер резилијентности и три компоненте сајбер резилијентности (Схема број 18: *Компоненте и категорије сајбер резилијентности*):

Категорије управљања ризиком

1) управљање;
2) идентификација;
3) заштита;
4) откривање;
5) одговор и опоравак.

Главне компоненте

1) тестирање;
2) ситуациона свесност;
3) учење и развој.

Схема број 18: ***Компоненте и категорије сајбер резилијентности***[388]

[388] *Guidance on cyber resilience for financial market infrastructures*, *op.cit.*, стр. 7.

Полазећи од важности сајбер резилијентности за предмет нашег истраживања, ми ћемо у наставку дати ближе објашњење садржаја оваквог приступа, где смо ради прегледности дали назив припадајућих категорија и компоненти, а тамо где смо сматрали да је корисно дали смо и ближе објашњење шта се подразумева под одређеном мером (Табела број 10: *Преглед садржаја компоненти и категорија сајбер резилијентности*).

Табела број 10: ***Преглед садржаја компоненти и категорија сајбер резилијентности***[389]

УПРАВЉАЊЕ	*Оквир сајбер резилијентности*	Утврђивање оквира сајбер резилијентности
		Сајбер је више од ИКТ-а (захтев је да се обухвате и људи и процеси)
		Управљање ризиком у организацији
		Екосистем фин. институције
		Међународни и домаћи стандарди
		Управљање конкретним ризиком
		Audits and Compliance ревизије и прегледи
	Улога Борда и вишег менаџмента	**Одговорности Борда** (да утврди оквир) и вишег менаџмента (да надгледа примену) сајбер резилијентности
		Култура (ниво свести о важности сајбер резилијентности у целој организацији)
		Вештине (Борд и виши менаџмент треба да имају чланове са потребним стручним знањима за сајбер резилијентност)
		Одговорност (потребно је одредити некога из вишег менаџмента ко је одговоран за сајбер резилијентност, а да има стручно знање, ауторитет, приступ Борду и друго)

[389] *Ibid*, стр. 9. – 22.

ИДЕНТИФИКАЦИЈА	*Идентификација и класификација*	Идентификација пословних функција и процеса
		Идентификација информационих добара
		Редовни преглед и ажурирање
	Повезаност	**Утицај на екосистем фин. институције свих учесника** (добављачи, друге банке, оператери телекомуникационих услуга, снабдевање енергијом и сл.)
ЗАШТИТА	*Заштита процеса и имовине*	**Контроле**
		Дизајнирање резилијентности (информациони ресурси повезани са критичним фукцијама треба да се ригорозно тестирају)
		Јаке ИКТ контроле: − Заштита информација − *Change management (управљање променама)* − *Безбедносна подешавања у складу са нивоом заштите*
		Слојевита заштита (сегментирање мрежа и критичних функција - да не буду повезани)
	Међуповезаност	Ризици повезаности система: − тако повезани да се уклапају у оквир сајбер резилијентности − оквир даваоца услуга треба да се уклопи у оквир рез. фин. институције
	Инсајдерске претње	***Безбедносна аналитика*** (откривање необичног понашања особа које имају приступ информационом систему, посебно критичним деловима, као и уклањање осетљивих података са мреже финансијске институције)
		Безбедносне провере приликом запошљавања (и повремене провере већ запослених)
		Контрола приступа (физички и логички приступ системима)
		Тренинг запослених фин. институције

	Тренинг	**Тренинг високоризичних група** (запослених са високим привилегијама приступа и осетљиве пословне функције)
ОТКРИВАЊЕ	*Откривање напада*	**Наставак мониторинга** (непрекидно праћење активности у реалном времену; формирање посебног Центра за отривање необичног понашања на мрежи)
		Свеобухватност мониторинга (познавање система и опасности које долазе од свих ентитета, укључујући тзв. *zeroday exploits - непознате претње и добављачима који су испоручили софтвер)*
		Слојевито откривање (подразумева претходну слојевиту заштиту којом су обухваћени људи, процеси и технологија. Један слој треба да прекрива и штити следећи. Треба настојати да су нападачу непознати наредни кораци у заштити)
		Одговор на инцидент
		Безбедносна аналитика
ОДГОВОР И ОПОРАВАК	*Одговор на инцидент, наставак активности и опоравак*	Планирање реакције
		Наставак акивности у оквиру 2 сата (2 сата *RTO*). Пресудно је да фин. Институција заврши процесе до краја дана
		Планирање ванредних ситуација
		Планирање и припрема
	Елементи дизајнирања	Уклапање у пословно окружење
		Интегритет података
	Међуповезаност	Уговори о дељењу података
		Спречавање ширења опасности
		Кризна комуникација
		Споразум о поверљивости

		Форензичка активност
ТЕСТИРАЊЕ	*Свеобухватни програм тестирања*	Програм тестирања
		Методологије и праксе: − Процена рањивости (*VA*) − Тестирање на основу сценарија − *Penetration* тестирање
		Тестирање од стране посебног тима (енгл: *Red team testing*)
	Координација	Координација
СИТУАЦИОНА СВЕСТ	*Обавештавање о претњи*	Идентификација потенцијалних претњи
		Процес истраживања опасности
		Прикупљање потребних података о претњи
		Ефикасна употреба информација
	Дељење информација	Планирање унапред
		Групе за размену информација
УЧЕЊЕ И РАЗВОЈ	*Учење у току догађаја*	Научене лекције из догађаја
		Стицање нових знања и способности
		Развијање предвиђања
	Упоређивање сајбер резилијентности (енгл: benchmarking)	Метрика

Наше је мишљење да овако приказана сајбер резилијентност одговара савременом разумевању области заштите информација у банкама и финансијским установама – посебно јер у оквиру сајбер заштите увиђа и неке претпоставке које смо изнели у хипотетичком оквиру нашег истраживања, а то је:

- заштита информација се не може сводити само на заштиту информатичких ресура, јер у себи треба да садржи и заштиту људи и процеса;
- заштита информација у себи садржи велики број мера које су нетехничке природе. Чак и приказаном моделу сајбер резилијентности, где је предмет заштите информациони систем финансијских институција, а не заштита информација у ширем контексту, можемо да видимо многе садржаје који по својој вокацији не припадају техничком сегменту (уско специјализована знања из области информационих технологија), већ су део менаџерских наука о управљању, планирању, о организационој култури, едукацији запослених и друго;

– на заштиту информационих ресурса односе се многе активности које се обављају у традиционално прихваћеном разумевању послова безбедности у организацији, обухватајући при томе области физичке и техничке заштите, безбедносне провере запослених и добављача, безбедносне истраге, безбедносне анализе и друго.

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

Након доношења Водича (или смерница, упутства) о сајбер резилијентности, Европска централна банка је у децембру 2018 године донела документ чија је намера да помогне у сагледавању стања које је остварено на основу акта (Водича) из 2016. године који смо претходно анализирали, те утврђивању даљих праваца развоја сајбер резилијентности – у даљем тексту, Документ о надгледању сајбер резилијентности (енгл: *Cyber resilience oversight expectations for financial market infrastructures – CROE*).[390]

Мотив за доношење оваквог документа је била чињеница да се од 2016. године примењује Водич за сајбер резилијентност, па се указала потреба да надлежни регулатори добију детаљније инструкције како би могли да сагледају и процене своје инфраструктуре финансијског тржишта у погледу поштовања резилијентности. У том контексту овај документ (*CROE*) има следеће кључне задатке:

– даје одговоре како операционализиовати смернице из Водича;
– омогућава регулаторима помоћ у процени сајбер резилијентности финансијског тржишта;
– пружа основу за дискусију између финансијских институција и регулатора.

Документ о надлегадању сајбер резилијентности препознаје три нивоа постигнућа резилијентности и то: почетни развој (енгл: *evolving*), даљи развој (енгл: *advancing*) и напредни ниво (енгл: *innovating*)

Полазећи од предмета истраживања нашег рада, и чењенице да смо претходно детаљно дали преглед мера које подразумева основни документ – Водич (смернице или упутства) о сајбер резилијентности, ми нећемо детаљно приказивати садржај документа о надгледању. Посебно, јер је *evolving* ниво практично дат у нашем прегледу и да је то довољно да сагледамо феноменологију сајбер резилијентности, а за будућа истраживања из ове области, дали смо извор из којег се може даље истраживати.

---

[390] Cyber resilience oversight expectations for financial market infrastructures, Europian cengtal bank, 2018., доступно на: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

Ипак, осећамо потребу, због доприноса нашем предмету истраживања, да направимо осврт на додатак који даје *CROE,* у односу на основни документ, а односи се на опис послова које треба да обавља виши извршни директор који је задужен за сајбер резилијентност.

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

У прегледу активности о сајбер резилијентности, које даје Водич, у делу где смо сагледали категорију *управљања* у овој области, и то приликом објашњења улоге Борда и вишег менаџмента, навели смо да се њихова одговорност састоји и у одређивању некога из вишег менаџмента ко би био одговоран за сајбер резилијентност у организацији, са условима да: има потребна стручна знања, да има потребан ауторитет у организацији и да има приступ Борду (због потребе честе комуникације).

Документ о надлегању сајбер резилијентности (*CROE*), доноси као додатак упутство о овој позицији у организацији, што се односи на наш предмет истраживања, па ћемо дати преглед овог додатка, према следећем:[391]

- финансијска институција треба да именује вишег руководиоца, обично руководиоца безбедности информација (енгл: *Chief information security officer – CISO*), који је одговоран за сва питања сајбер резилијентности у финансијској институцији, укључујући и одговорност трећих лица. Виши извршни директор се стара о извршењу мера које су одређене сајбер стратегијом финансијске институције;
- виши иизвршни директор или *CISO* извршава следеће задатке:
  i. подршка вишем руководству и Борду приликом дефинисања и ажурирања политике сајбер резилијентности и саветовање о свим питањима која су с тим у вези. Ово укључује и помоћ у решавању сукобљених интереса, као што је на пример *економичност* у односу на сајбер резилијентност;
  ii. учествовање у управљању сајбер ризиком;
  iii. израда смерница за сајбер резилијентност и, према потреби, било којих других правила из ове области, као и провера поштовања;
  iv. утицај на процесе сајбер резилијентности финансијске институције, надгледање IT услуга, провајдера и помоћ у било којим сродним задацима;
  v. помагање у изради и ажурирању плана за кризне ситуације у вези са сајбер питањима;
  vi. иницирање и праћење спровођења мера сајбер резилијентности;
  vii. учествовање у пројектима релевантним за сајбер резилијентност;
  viii. делује као контактна тачка за сва питања која се тичу сајбер резилијентности која долазе из финансијске институције или од трећих лица;

[391] *Ibid*

ix. истраживање сајбер индидената и извештавање о њима вишем руководству и Борду;
x. континуирано истраживање претњи које се односе на *IT* ресурсе;
xi. иницирање и координација мера за подизање свести о сајбер резилијентности и спровођење обука;
xii. извештавање вишег руководства и Борда редовно, најмање квартално, као и *ad hoc* на основу статуса сајбер резилијентности. Овај статус укључује, на пример, процену стања сајбер резилијентности у поређењу са претходним извештајем, информације о пројектима из ове области, сајбер инциденте и резултате спроведених тестова продора и тестова *црвених тимова* (енгл: *red team*).

– у погледу организације и процеса, виши извршни директор или *CISO*, мора бити независан како би избегао било какве потенцијалне сукобе интереса. Из тих разлога очекује се:

i. организација која ће осигурати да ова функција може да делује независно од *IT*-а, и да може да извештава више руководство и Борд у било које време. Такође, очекује се да ова функција није укључена у пословну функцију Интерне ревизије;
ii. одређивање потребних ресурса које он захтева;
iii. одређивање буџета за обуке за сајбер резилијентност у финансијској институцији и за даљу обуку вишег извршног особља и за чланове његовог тима;
iv. захтев да се пријаве било који инциденти релевантни за сајбер резилијентност;

– финансијска институција треба да има на овој позицији сопственог запосленог, у зависности од специфичности њене структуре и организације. У мери у којој то дозвољава национални регулатор и у случајевима великих система може се поставити *CISO* за целу групу.

Полазећи од свега наведеног, мишљења смо да допунска објашњења издата од стране Европске централне банке дају ближа објашњења и помажу у разумевању сајбер резилијентности финансијских институција, а посебно да могу бити корисна у евентуалном практичној примени резултата нашег истраживањања, у погледу организовања послова заштите информација у банкама и финансијским институцијама.

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

У издању Групације светске банке, 2019. године, објављен је преглед новијих закона, прописа, смерница и других значајних докумената о кибернетичкој безбедности за финансијски сектор.

Иако се Међународна банка за обнову и развој (енгл: *International Bank for Reconstruction and Development – IBRD*) често сматра синонимом за Светску банку, она је само једна, додуше стожерна организација Групације светске банке (енгл: *World Bank Group*), поред: Међународног удружења за развој, Међународне финансијске корпорације, Мултилатералне агенције за гарантовање инвестиција и Међународног центра за решавање инвестиционих спорова.[392]

Групацију светске банке не треба мешати са Светском банком. Групацију светксе банке чине пет интернационалних организација. *IBRD* и Међународно удружење за развој (енгл: *International Development Association – IDA*) понекад се колективно називају *Светска банка*.

Будући да овај документ пружа слику о изабраној компилацији прописа који се односе на нашу област истраживања (није свеобухватни попис свега што су објавиле све јурисдикције и међународна тела), а да смо ми у досадашњем раду већ истакли оне документе за које смо сматрали да су важни за предмет истраживања у нашем раду, сматрамо да је корисно, посебно за будућа истраживања, да прикажемо преглед и неких других докумената која су корисна за изучавање заштите информација у банкама и финансијским институцијама. [393]

EU Cybersecurity Act (април, 2019. године), Европски савет је усвојио Закон о кибернетичкој сигурности ЕУ. Закон даје трајни мандат Агенцији Европске уније за безбедност мреже и информација (ЕНИСА) као европској Агенцији за кибернетичку сигурност и успоставља оквир сертификовања о кибернетичкој сигурности ЕУ.[394]

Joint Advice on the costs and benefits of a coherent cyber resilience testing framework (април, 2019. године), Европска надзорна тела (енгл: *European Supervisory Authorities − ESAs*) објавили су заједничко саветовање о трошковима и предностима кохерентног оквира за тестирање на сајбер резилијентност за значајне учеснике на тржишту и инфраструктуру унутар читавог финансијског сектора ЕУ.[395]

---

[392] Миленковић, И.: *Групација светске банке (енгл: World bank Group)*, часопис Економски погледи, број 3/2009, 2009. година, стр. 108. – 109. Доступно на: http://www.efpr.edu.rs/Ekonomski%20pogledi/3-2009%20PDF/10.pdf

[393] *Financial Sector's Cybersecurity*: *A Regulatory Digest*, World Bank Group, 2019., доступно на: http://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf

[394] Доступно на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[395] *Joint Advice on the costs and benefits of a coherent cyber resilience testing framework*. Доступно на: https://www.esma.europa.eu/sites/default/files/library/jc_2019_25_joint_esas_advice_on_a_coherent_cyber_resilience_testing_framework.pdf

Joint Advice on the need for legislative improvements relating to ICT risk management requirements (април, 2019. године), Европска надзорна тела (енгл: *European Supervisory Authorities − ESAs*) објавили су заједничко саветовање о потреби за законодавним побољшањима која се односе на захтеве управљања ризиком у вези са информационом и комуникацијском технологијом (ИКТ) у финансијском сектору Европске уније (ЕУ).[396]

EBA Guidelines on outsourcing arrangements (фебруар, 2019. године), Европски банкарски орган (енгл: *The European Banking Authority − EBA*) објавио је завршни извештај о смерницама о аранжманима за *outsorcing*, утврђујући посебне одредбе за оквире управљања свих финансијских институција у оквиру мандата ЕБА у погледу њихових аранжмана за *outsorcing* и с тим у вези повезаних очекивања и процеса надзора.[397]

Cyber Europe 2018 After Action Report (децембар, 2018. године), ЕНИСА (енгл: *European Union Agency for Cybersecurity − ENISA*) је објавила свој извештај о вежби кибернетске безбедности у целој Европи. Ово извођење двогодишње вежбе од стране ЕНИСА-е било је усмерено на ваздухопловну индустрију, али је ипак реч о критичној инфраструктури, па је у том смислу корисно погледати документ, са аспекта нашег предмета истраживања.[398]

Crisis communication exercise report (децембар, 2018. године), Комитет за тржишну инфраструктуру и платна средства Еуросистема (енгл: *Eurosystem's Market Infrastructure and Payments Committee – MIPC*), извршио је тржишну вежбу кризне комуникације на целом тржишту крајем јуна 2018. године и објавио о томе извештај у коме су резимирани циљеви вежбе, сценарио, кључни закључци и наредни кораци.[399]

Cyber Lexicon (новембар, 2018. године), ФСБ (енгл: *Financial Stability Board − FSB*) је објавио Сајбер лексикон, који садржи скуп од око 50 основних израза који се односе на сајбер безбедност и сајбер резилијентност у финансијском сектору. У одређивању тумачења појмовника коришћени су бројни међународни стандарди, укључујући стандарде издате од стране Међународне организације за стандардизацију (енгл: *International Organization for Standardization − ISO*), Удружење за ревизију и контролу информационих система (енгл: *Information Systems Audit and Control Association − ISACA*), САНС институт (званични назив је *Escal Institute of Advanced Technologies*, а акроним SANS је од *SysAdmin, Audit, Network*

[396] *Joint Advice on the need for legislative improvements relating to ICT risk management requirements*. Доступно на: https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

[397] *EBA Guidelines on outsourcing arrangements*, доступно на: https://eba.europa.eu/sites/default/documents/files/documents/10180/2761380/78acbfce-18e9-4f4a-8460-717542b3fd34/EBA%20revised%20Guidelines%20on%20outsourcing_HR.pdf

[398] *Cyber Europe 2018 After Action Report*, доступно на: file:///C:/Users/windows%207/Downloads/2017-27-06%20CE2016%20After%20action%20report.pdf

[399] *Cyber Europe 2018 After Action Report*, доступно на: https://www.ecb.europa.eu/pub/pdf/other/ecb.unitasreport201812.en.pdf

and Security) и амерички Национални институт за стандарде и технологију (енгл: *U.S. National Institute of Standards and Technology −NIST*).[400]

Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector (октобар, 2018. године), Владе Групе 7 (Г7) објавиле су Основне елементе за управљање сајбер ризиком трећих страна у финансијском сектору. Раније је Г7 у октобру 2016. године, објавила Основне елементе кибернетичке сигурности за финансијски сектор (енгл: *Fundamental Elements of Cybersecurity for the Financial Sector*), а Основне елементе за ефикасну процену кибернетске сигурности у финансијском сектору (енгл: *Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*), у октобру 2017. године.[401]

*TIBER-EU Framework Services Procurement Guidelines (*мај, 2018. године) Европска централна банка објавила јединствени оквир за контролисано тестирање сајбер резилијентности субјеката финансијског тржишта. Сродне смернице, за набавку услуга уследиле су у августу. Документ омогућава хармонизовани европски приступ тестирањима који опонашају тактике, технике и поступке правих хакера који могу бити права пријетња (тзв. *Red team*). Тестови засновани на ТИБЕР-у ЕУ симулирају сајбер напад на критичне функције ентитета, укључујући људе, процесе и технологије. [402]

Не наводећи даље нормативу која се односи на заштиту информација у банкама и финансијским установама, сматрамо да можемо да закључимо да је активност на овом пољу у свету врло развијена (ми смо у овом делу дали преглед само дела докумената која су донета од 2018 до данас), и да ће временом постати, исто као и претње, још израженија. За будућа истраживања на овом пољу, навели смо извор наших података, будући да је реч о периодици коју издаје Групација светске банке, како смо претходно навели. Иако нормативни оквир није још увек обавезујући, посебно не за домаће банке, мишљења смо да је корисно сагледати и овај аспект у остваривању заштите информација у банкама и финансијским институцијама, како смо то ми учинили, будући да очекујемо да регулатор у скоријој будућности направи напоре ка хармонизацији домаћег банкарског амбијента у области заштите информација, сагласно трендовима у развијеном свету.

[400] *Cyber Lexicon*, Financial Stability Board (FSB), 2018. Доступно на: https://www.fsb.org/wp-content/uploads/P121118-1.pdf

[401] *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*, доступно на: https://www.bundesbank.de/resource/blob/764692/01503c2cb8a58e44a862bee170d34545/mL/2018-10-24-g-7-fundamental-elements-for-third-party-cyber-risk-data.pdf

[402] *TIBER-EU Framework Services Procurement Guidelines*, European Central Bank, доступно на: https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf

7. Међународни стандарди у остваривању заштите информација

Концепт заштите информација је очигледно много више од примене савремених техничких решења које нуде информационе технологије, што је потврђено развојем бројних међународних стандарда у овој области.

У току нашег истраживања на више места смо навели да се поједини аутори, у зависности од времена настанака њиховог истраживања, позивају на одговарајуће стандарде, па смо тако наводили да су стандарди од суштинске важности за самоучење стручњака (ми би рекли и од додатне важности за самоучење стручњака на овим просторима, будући да су овдашњи образовни програми углавном усмерени ка техници или нетехници, и не заснивају се на безбедносној науци као фундаменту, са додатним изучавањем других елемената који чине област заштите информација, укључујући менаџерске и друге науке и стручна знања, као и област стандардизације).

Бројни су и научни радови који истражују проблем неопходне документације за успостављање безбедносне политке у организацији, о чему не постоје јединствени ставови о устројству безбедносне документације, али је примећено и да те разлике нису суштинске а да приступ зависи од контекста, односно од конкретних услова организацијског амбијента.

Кинари наводи да су стандарди документа која по приоритету прате безбедносне политике, с тим да се некада наводи да им претходе смернице, односно процедуре, што јесте мањински став, али да он зависи од конкретне организације, нормативног амбијента, безбедносне културе организације и другог.[403]

У домаћем нормативном оквиру, наводи се да ради одржавања безбедности система морају да се спроводе различите мере, као и примењивање нових техничких и програмских средстава у систему, у складу са стандардима СРПС ИСО/ИЕЦ 27001 и СРПС ИСО/ИЕЦ 17799.[404]

Реч је о фамилији међународних стандарда која је данас најчешће у употреби, одакле ћемо дати ближе објашњење ове групе стандарда, које је издала Међународна организација за стандардизацију (енгл: *International Organization for Standardization – ISO*), и који се односе на менаџмент система за сигурност информација (енгл: *Information security management system – ISMS*).[405]

---

[403] *Development of a Structured Security Document Framework*, Kinnari Johana, Laurea University of Applied Sciences, Master's Thesis, Vantaa, Finland, 2013. Доступно на: https://www.theseus.fi/bitstream/handle/10024/57628/Kinnari_Johanna.pdf;jsessionid=7599D39C85C7600A43B55B320B786B8B?sequence=1

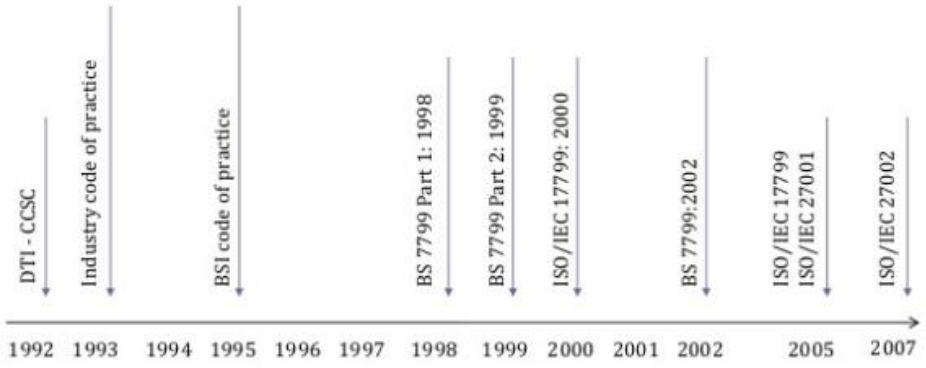
[404] Уредба о посебним мерама заштите тајних података у информационо-телекомуникацијским системима, Службени гласник РС, број 53/11, Члан 10

[405] *ISO* уско сарађује са Међународном електротехничком комисијом (енгл: *International Electrotechnical Commission – IEC*) по питањима електротехничке стандардизације

Група међународнх стандарда за управљање безбедношћу информација (енгл: *Information Security Management System – ISMS*) чини оквир којим организације могу да управљању заштитом својих информационих система, а који је настао развојем ранијих (британских) стандарда из ове области (Графикон број 14: *Преглед историје развоја стандарда за управљање безбедношћу информација до увођења стандарда ISO 27001*).

ISMS се састоји од политика, процедура, смерница и повезаних ресурса и активности, којима управља организација у циљу заштите својих информација. Представља систематски приступ за успостављање, спровођење, рад, праћење, преглед, одржавање и побољшање информационе сигурности организације за постизање пословних циљева.

Графикон број 14: ***Преглед историје развоја стандарда за управљање безбедношћу информација до увођења стандарда ISO 27001***[406]



Група међународнх стандарда за управљање безбедношћу информација (*ISMS*), заснована је на процени ризика и нивоима прихватања ризика путем анализе заштите информационих средстава и примени одговарајућих контрола. Основна начела која доприносе примени *ISMS*-а, дата су према следећем:[407]

- свест о потреби информационе сигурности;
- одређивање одговорности за сигурност информација;
- посвећеност менаџмента и интереса заинтересованих страна;
- развој одговарајућих вредности у организацији према заштити информација;
- процена ризика којима се одређују одговарајуће контроле како би се достигао прихватљив ниво ризика;
- прихватање безбедности као битног елемента информационих мрежа и система;
- активно спречавање и откривање инцидената у заштити информација;

[406] Извор: https://www.slideshare.net/Businessbeamltd/what-is-iso-27001-isms

[407] Извор: *International standard ISO/IEC 27000:2018*, стр. 11. – 12. Доступно на: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

- свеобухватан приступ у управљању заштите информација;
- континуирано преиспитивање заштите информација и уношење потребних измена.

Према ISO 27000 безбедност информација обезбеђује поверљивост, доступност и интегритет информација, што укључује примену и управљање одговарајућих контрола, с циљем да се обезбеди континуитет и минимизирање последица инцидената. Остварује се применом низа контрола кроз процес управљања ризиком, укључујући политике, процесе, процедуре, организационе структуре, софтвер и хардвер за заштиту информатичких ресурса.[408]

Фактори који су пресудни за успешну имплементацију *ISMS*-а су следећи:[409]

- политике, циљеви и активности информационе безбедности морају да буду усклађени са општим циљевима организације;
- приступ, спровођење, надледање, одржавање и унапређење заштите информација треба бити *у складу са организационом културом*;
- посвећеност менаџмента, а посебно највишег менаџмента мора бити видљива;
- разумевање захтева за заштитом информационих ресурса мора бити у складу са ISO/IEC 27005;
- програми обуке за развој свести (енгл: *security awareness*) за све запослене, и друге релевантне учеснике, треба да садрже обавезе које су утврђене одговарајућим безбедносним политикама и стандардима и да мотивишу учеснике да поступају по њима;
- потребам је ефикасан процес управљања инцидентима у области заштите информација;
- потребан је ефикасан приступ управљању континуитетом пословања;
- потребан је одговарајући систем мерења за процену перформанси у управљању заштитом информација који ће давати и повратне сугестије за побољшање.

Породица *ISMS*-а (Схема број 19: *Приказ ISMS групе стандарда*) састоји се од међусобно повезаних стандарда који се стално развијају (неки су тек планирани да се донесу) и садрже структурне компоненте које су садржане у стандарду ISO/IEC 27001 као и у стандарду захтева цертификационог тела код потврђивања сагласности са овим стандардом, ISO/IEC 27006, и – додатног оквира за специфичан сектор ISO/IEC 27009.

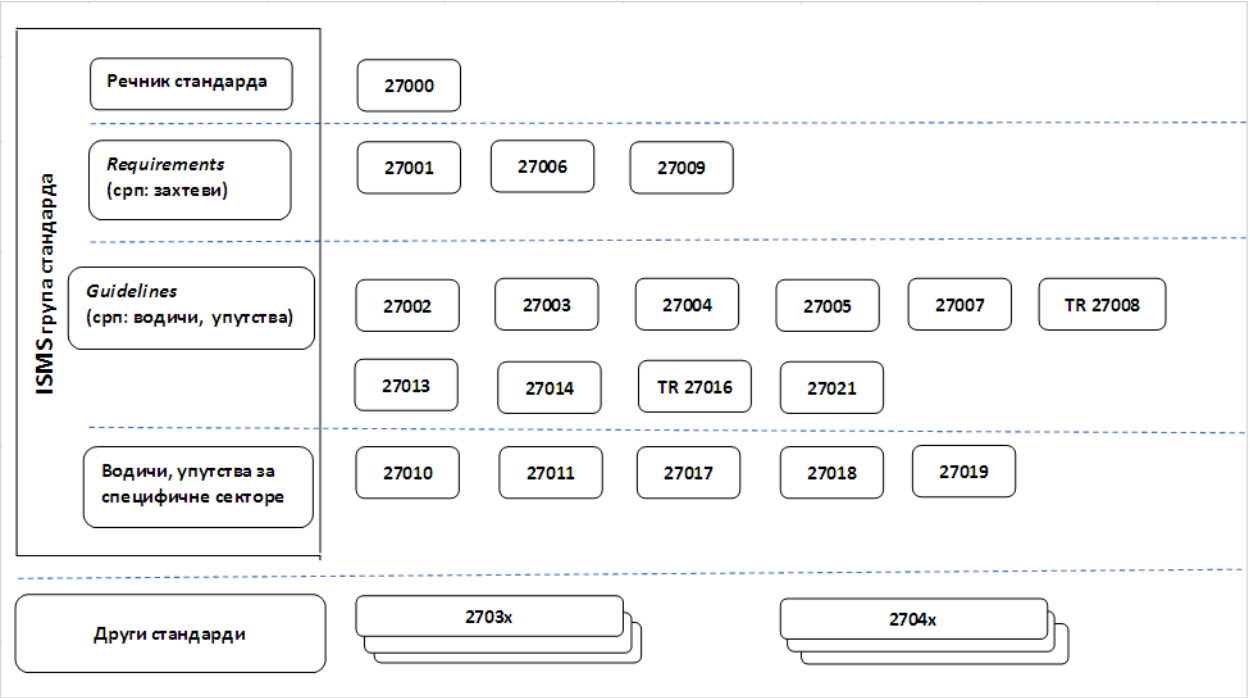
Остали документи дају смернице за различите аспекте имплементације *ISMS*-а.

ISO/IEC 27001 прецизира захтеве за успостављање, примену, рад, праћење, преглед, одржавање и побољшање формалиованих система управљања сигурношћу информација (*ISMS)* у контексту укупних пословних ризика организације. Одређује захтеве за примену контрола безбедности информација прилагођених потребама појединих организација или

[408] *Ibid*
[409] *Ibid,* стр. 17.

њихових делова, и у том смислу је универзалан, без обзира на њихову врсту, величину и природу.[410]

Схема број 19: ***Приказ ISMS групе стандарда***[411]



ISO/IEC 27002 представља кодекс праксе за контролу информационе безбедности и као такав пружа списак опште прихваћених контролних циљева и најбоље праксе контроле које ће се користити као водич (или упутство) при избору и примени контрола. Од 2007. године представља дотадашњи стандард ISO/IEC 17799. [412]

Поред наведених стандарда, други стандарди из серије дати су према следећем:[413]

– ISO 27003, водич за имплементацију система за управљање информацином безбедности;

[410] *Ibid*, стр. 20.
[411] *Ibid*
[412] Извор: *International standard ISO/IEC* 27002:2005, доступно на: http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27002.pdf
[413] Шеховић, Д.: *Стандарди за управљање информационим системима финансијских институција*, мастер рад, Универзитет Сингидунум, Београд, 2014., стр. 32. - 33., доступно на: https://singipedia.singidunum.ac.rs/izdanje/41325-standardi-za-upravljanje-informacionim-sistemima-finansijskih-institucija; Вуксановић, Д.: Стандарди у области безбедности ИКТ, Институт за стандардизацију Србије, Београд, 2017., доступно на: https://coming.rs/wp-content/uploads/2017/09/Standardi-u-oblasti-bezbednosti-IKT-a.pdf

- ISO 27004, мерење и метрике ефикасности система информационе безбедности;
- ISO 27005, управљање ризицима информационе безбедности;
- ISO 27006, захтеви за поступком анализе и сертификовања стандарда;
- ISO/IEC 27007, смернице за ревизију управљања безбедношћу информационих система;
- ISO/IEC 27011, смернице за управљање информационом безбедношћу телекомуникационих организација;
- ISO/IEC 27014, управљање безбедношћу информација;
- ISO/IEC TR 27015, смернице за менаџмент безбедношћу информација за финансијске услуге
- ISO/IEC 27033, преглед и концепти безбедности у мрежама;
- ISO/IEC 27799, управљање безбедношћу информација у здравству;

На област заштите информација односе се и бројни други стандарди изван серије ISO 27000, као што су: SRP ISO 22301, Друштвена безбедност - Системи менаџмента континуитетом пословања – захтеви; SRPS EN ISO 22313, Друштвена безбедност – систем менаџмента континуитетом пословања – упутство и SRPS EN 31010, менаџмент ризиком – технике оцене ризика.[414]

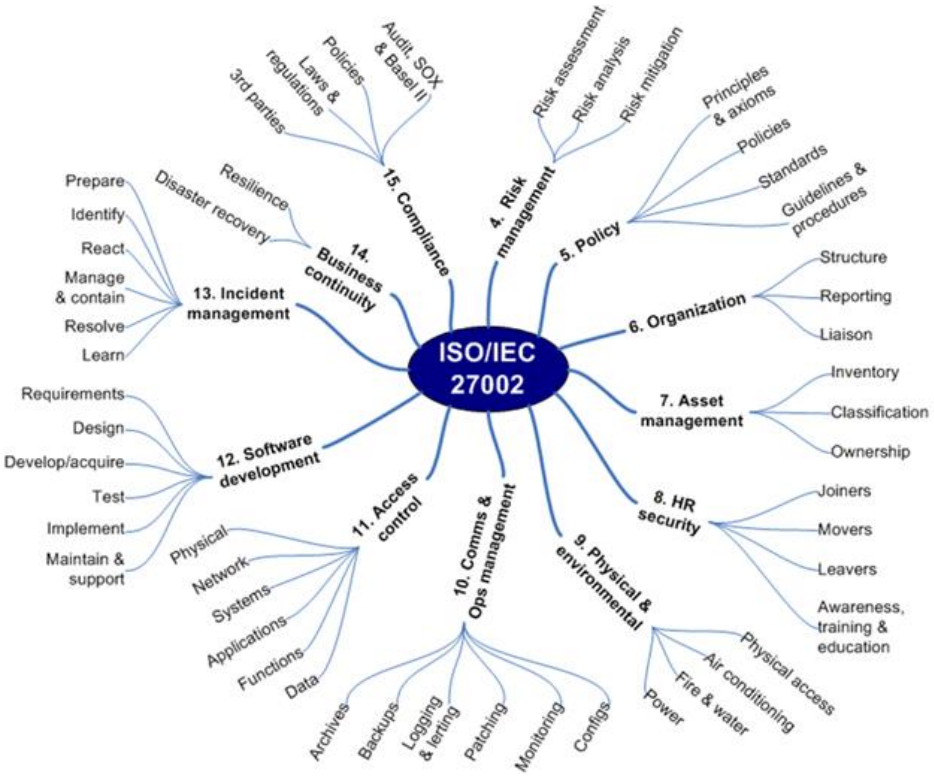
Стандард ISO/IEC 27002 је од значаја за предмет истраживања нашег рада, будући да обухвата области према следећем (Схема број 20: *Садржај стандарда ISO/IEC 27002*)[415]

- безбедносну политику;
- организовање заштите информација;
- управљање информацијама као ресурсом;
- *HR* безбедност;
- физичку безбедност;
- управљање комуникацијама и операцијама;
- контролу приступа;
- набавку, развој и одржавање информационих система;
- управљање инцидентима у заштити информација;
- управљање континуитетом пословања;
- усклађеност (енгл: *compliance*).

Организовање заштите информација и законска усклађеност представљају области стандарда ISO/IEC 27002 које се односе на организационо и нормативно уређење заштите информација, због чега ћемо дати детаљнији осврт на ове делове стандарда.

[414] Вуксановић, Д., *Ibid.*
[415] *International standard ISO/IEC* 27002:2005, стр. 4.

Схема број 20: ***Садржај стандарда ISO/IEC 27002***[416]



Стандард наводи да пословодство треба да одобри политику заштите информација додељујући безбедносне улоге у организацији и да том приликом треба да координира имплементацију безбедности широм организације. Уколико је потребно, треба да се успостави стручни савет за заштиту информација, укључујући спољашње сараднике, како би се пратили трендови и стандарди у индустрији безбедности. Посебно, пословодство треба да подстиче мултидисциплинарни приступ у информационој безбедности.[417]

Менаџмент треба да:

- осигура да се утврде циљеви информационе безбедности и да се имплементирају у релевантне пословне процесе у целој организацији;
- формулише, прегледа и одобри политику информационе безбедности;
- прати ефикасност примене утврђене политике;
- пружа јасан правац и видљиву подршку менаџменту за спровођење безбедносних иницијатива;
- обезбеди потребне ресурсе за безбедност информација;
- одређује потребне улоге и одговорности за заштиту информација широм организације;

[416] F. Alcazar, S. Fenz, *Mapping ISO 27002 into Security Ontology*, Vienna University of Technology, стр. 5., доступно на: https://upcommons.upc.edu/bitstream/handle/2099.1/17302/memoria.pdf?sequence=4&isAllowed=y
[417] Ibid, стр. 9.

- иницира програме и планове за развој свести о безбедности;
- осигура примену одговарајућих безбедносних контрола у целој организацији;

Менаџмент треба и да идентификује потребе за интерним или екстерним стручним саветима за информациону безбедност, што подразумева и формирање посебних савета, у зависности од величине организације.

Поред наведеног, у склопу интерних активности, стандард обухвата и следеће теме:

- координацију информационе безбедности;
- расподелу одговорности за информациону безбедност;
- процес ауторизације за информационе системе;
- споразуме о поверљивости;
- контакте са надлежним регулаторима;
- контакте са одговарајућим интересним групама;
- независну ревизију система информационе безбедности.

Када је у питању деловање менаџмента према спољашњим чиниоцима информационе безбедности, њихове обавезе се састоје у следећем:

- идентификацији информацијских ризика повезаних са пословним сарадницима;
- одређивање безбедносних захтева пре сарадње са пословним сарадницима;
- третирању безбедноси у споразумима са трећим странама.

У вези са законском усклађености (енгл: *compliance*), стандард поставља за циљ да се избегне кршење било ког закона, регулаторних или уговорних обавеза и било који други безбедносни захтеви, којом приликом треба имати у виду различиту законодавну праксу.

У том смислу, стандард као посебне области издваја: усаглашеност са законским захтевима; усаглашености са безбедносним политикама и стандардима; и − питања ревизије информационих система.[418]

Овај стандард и у другим сегментима доприноси предмету нашег истраживања, које нећемо због ограничености простора да посебно разматрамо, али напомињемо да ове одредбе могу бити корисне за будућа истраживања различитих аспеката заштите информација (као што су области HR безбедности, где су обухваћени програми за развој безбедносне свести, безбедносне провере запослених, безбедносне политике приликом одласка запослених, дисциплинске мере и друго; физичка безбедност; континуитет пословања итд.).

Друге стандарде из групе која уређује менаџмент система за сигурност информација (*ISMS*) нећемо посебно разматрати, будући да се не односе на наш предмет истраживања у мери као претходно наведени (ISO 27000, ISO 27001 и ISO 27002), са напоменом да је преглед

[418] *Ibid*, стр. 100. – 106.

објављевних стандарда јавно доступан за будућа истраживања у области заштите информација, као и да се радови са овом тематиком релативно често објављују.[419]

Такође, напомињемо да се у области заштите информација користе и други стандарди, али да смо се за потребе нашег истраживања определили да прикажемо серију стандарда из породице ISO 27000, будући да су они најраспрострањенији. У том смислу за будућа истраживања могу користити стандарди, као што су: *COBIT* (енгл: *Control Objectives for Information and Related Technology*[420]), који се користи углавном у финансијској индустрији; серије стандарда које је издао Амерички национални институт за стандарде и технологију (енгл: *US National Institut of Standards and Technology – NIST*)[421]; специфичпни стандарди за одређену индустрију, као што је *PCI DSS* (енгл: *Payment Card Industry Data Security Standard*)[422], основни стандард у индустрији платних картица; Уредба Европског парламента о заштити појединаца у вези са обрадом личних података и слободном кретању таквих података (енгл: *General Data Protection Regulation – GDPR*)[423] и бројни други.

8. Закључна раматрања поглавља

Нормативно уређење области заштите информација у банкама и финансијским институцијама представља обимну област истраживања и засновано је на прописима државних органа, специфичним законима и подзаконским актима које доноси регулатор ове области, Народна банка Србије, међународним стандардима, смерницама, упутствима, препорукама најбоље праксе, као и интерним актима банака и финансијских институција.

Устав републике Србије сврстава неповредивост тајности писма и друге комуникације и заштиту података о личности у основна људска и мањинска права и представља основ за доношење закона којима се детаљније уређује начин остваривања људских права и права која у овој области имају правна лица.

Закон о тајности података (2009), Закон о заштити података о личности (2009), Закон о заштити пословне тајне (2011), Закон о слободном приступу информацијама од јавног значаја (2004), представљају скуп релевантних закона којима се регулише обрада и заштита одређених врста података, чије нормативно уређење држава сматра неопходним и целисходним. У том смислу најважније врсте података су: тајни подаци, подаци о личности, информације од јавног значаја, пословне тајне и професионалне тајне. Поред наведеног, постоје и други прописи који појединим одредбама пружају правну заштиту неким категоријама података, као што су: *Кривични законик, Службени гласник РС, 2005; Законик о кривичном поступку, Службени гласник РС, 2011; Закон о информационој безбедности,*

[419] Преглед свих стандарда серије ISO 27000, са називом, датумом издања и описом подручја примене доступан је на линку: https://www.iso27001security.com/ISO27k_Standards_listing.pdf
[420] Извор: https://www.isaca.org/bookstore/cobit-5/wcb5dmp
[421] Извор: https://www.nist.gov/cyberframework
[422] Извор: https://www.pcisecuritystandards.org/pci_security/
[423] Извор: https://gdpr-info.eu/

Службени гласник РС, 2016; Закон о привредним друштвима, Службени гласник РС, 2011; Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, 2005).[424]

У нашем истраживању ми смо приказали Закон о тајности података и подзаконске прописе из ове области, где су предвиђени одређени услови да би податак постао тајни, односно приказали смо да је потребно да постоји правни основ и да се спроведе поступак одређивања тајности података. У том смислу податак може да има један од следећих степена тајности:

- државна тајна (неотклоњива тешка штета по интересе Републике Србије);
- строго поверљиво (тешка штета по интересе Републике Србије);
- поверљиво (штета по интересе Републке Србије);
- интерно (спречавање могућности настанка штете за рад, обављање задатака и послова органа јавне власти који их је донео).

Да би неко физичко или правно лице добило приступ тајном податку потребно је да се испуне законски услови (издавање цертификата, претходна безбедносна провера и друго).

Закон о заштити пословне тајне (Сл. Гласник РС, бр. 72/11) регулише правну заштиту пословне тајне од радњи нелојалне конкуренције.

Пословна тајна је било која информација која има комерцијалну вредност зато што није опште позната, нити је доступна трећим лицима која би њеним коришћењем или саопштавањем могла остварити економску корист, и која је од стране њеног држаоца заштићена одговарајућим мерама у складу са законом, пословном политиком, уговорним обавезама или одговарајућим стандардима у циљу очувања њене тајности, а чије би саопштевање трећем лицу могло нанети штету држаоцу послове тајне.[425]

Мере заштите пословне тајне могу бити:

- физичко-техничке;
- административне;
- персоналне;
- информационе.

Закон о заштити података о личности (Сл. гласник РС, 97/08, 104/09, 68/12 и 107/12) регулише област обраде података о личности, заштиту права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним судом за заштиту података о личности, као и друга питања.[426]

[424] Мандић, Г. Ј., Путник, Н., Милошевић, М., *op.cit.,* стр. 223.

[425] *Ibid*

[426] *Ibid,* стр. 249. – 265.

Овим актом одређени су појмови: руковалац података, обрађивач података, корисник података, збирка података, Централни регистар збирке података коју води Повереник, и – категорија нарочито осетљивих података о личности (национална припадност, раса, пол, језик, вероисповест и друго).

Закон о ифнормационој безбедности (2016. године) одређује да се овим актом уређују мере заштите од безбедносних ризика у ИКТ системима, одговорности правних лица приликом управљања и коришћења ИКТ система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.[427]

Законом је информациона бебедност одређена као *скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост подататка*, да би тај систем функионисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.

Члан 16 Закона одређује *финансијске институције као делове ИКТ система од посебног значаја*, услед чега се на њих примењују посебне мере заштите.

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, (2016.), одређује мере заштите ИКТ система од посебног значаја. Оператери су добили обавезу израде Акта о безбедности ИКТ система од посебног значаја, а обавеза је конретизована доношењем одговарајућег акта (*Уредба о ближем садржају акта о безбедности информационо-комуникацијског система од посебног значаја, начину провере и садржају извештаја о провери безбедносно-инфорамционог система од посебног значаја 2016.*)

Извештавање о инцидентима (Члан 11) регулисано је доношењем *Уредбе о поступку достављања података, листи, врстама и значају инцидента и поступку обавештавања о инцидентима у информационо-комуникацијским системима од посебног значаја (2016.)*.

Успостављање Националног центра за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ), Закон је прописао у Члановима 14 и 15.

Национални центар за превенцију безбедносних ризика у ИКТ системима Републике Србије основан је у оквиру Регулаторне агеницје за телекомуникације и поштанске услуге.

Интерни правни акти спадају у домен недржавног или аутономног права. Унутрашња правна регулатива представља механизам у области *менаџмента ризика*.

Предузећа на овај начин самостално уређују питања процене, превенције и контроле ризика која нису регулисана државним правним актима или примењују законске норме, прилагођавајући их специфичностима сопствене организације, структуре, делатности и система пословања. На тај начин унутрашњи правни акти могу да надокнаде недостатке спољне регулативе и могу да створе оптималан систем за спровођење законских обавеза. То

[427] *Ibid,* стр. 265. – 274.

је процес инструментализације правних овлашћења организације за сврхе менаџмента кризе.[428]

Непостојање унутрашње нормативне регулативе може се окарактерисати као правни ризик, који се у вези са пословањем банака и финансијских институција наводи у оквиру међународних споразума означених као – Базел споразуми.

Национални стандард за процену ризика у заштити лица, имовине и пословања (СРПС Ал2:003.2008.) је поставио критеријуме за идентификацију и оцену правних ризика, према којима у организацији треба да постоји: адекватна регулатива којом се смањује могућност одавања тајних података, података о личности и других штићених података; адекватна регулатива којом се предвиђа одговорност лица због непоштовања интерних процедура које су могле или које су проузроковале негативне имовинске или неимовинске последице по корисника; адекватна регулатива којом се смањује опасност од неадекватног мониторинга судских, управних и других спорова, и – адекватна регулатива којом се смањује могућност наступања пропуста у процесу обезбеђења који су наступили услед неадекватне интерне регулативе.

У интерне акте правног лица убрајају се: статут, правилници, одлуке, пословници и други акти, као и процедуре и упутства.[429]

Значај интерне регулативе огледа се у заштити пословне тајне, јер ова материја јесте дефинисана законом и другим прописима, али је и остављен простор за организације да интерним актима ближе регулишу поједина питања, и на тај начин додатно се заштите у односу на изворе угрожавања у овом смислу. Такође, законска заштита може да се активира тек уколико је присутна интерна регулатива заштите пословне тајне.

Правилник о пословној тајни, разрађују сва питања у вези са поверљивим пословним информацијама и омогућава успешну заштиту организације у том смислу. Намена овог документа јесте да одреди документа и информације које, у складу са законима и највишим правним актом правног лица, представља пословну тајну, а истакнуто је да сва лица (запослени и пословни сарадници) треба да буду упонати са овим актом и да о истом питпишу *Изјаву о чувању пословне тајне*. У домаћој пословној пракси за овај документ се често користе називи на енглеском језику, као што су: *Non-Disclosure Agreement (NDA), Confidetiality Agreement (CA), Confidental Disclosure Agreement (CDA), Proprietary Informaton Agreement (PIA) i Secrecy Agreement (SA).*

Правилник о приватности, или Одлуку о поступку приликом прикупљања, обраде и евиденције података о личности, интерно се уређује начин поступања запослених приликом наведених радњи.

[428] *Ibid.*
[429] *Ibid*, стр. 278.

Препорука је да организација донесе *Политику заштите података о личности*, где се прецизира да организација врши обраду неопходних података оних лица која су дала пристанак за обраду.[430]

Надлежни орган одређује решењем лице задужено за координацију активности у погледу чувања, обраде и прикупљања података о личности и испуњавања законских обавеза, укључујући формирање и пријављивање збирки података о личности и предузимање организационо-техничких мера за заштиту података.[431]

Интерна безбедносна документата омогућавају да се поштују правила која долазе из спољашњег окружења организације и одражавају ставове организације о одређеним питањима и одређују начине како ће организација да постигне циљеве за које се определила. На основу усвојене политике доносе се безбедносна правила која се уобличавају у писани документ. Потребно је запослене упонати са садржајем, урадити едукацију (тренинг), одредити и применити контролне активности за примену правила, одредити вредности које се прате као би мерили ефикасност спровођења утврђеног правила, што треба да представља континуирани процес који се базира на развоју свести запослених о безбедносним потребама организације.

Како ће се људи односити према прописаним мерама заштите зависи од организационих, нормативних, техничких мера, а у првом реду зависи од стања свести о безбедности (енгл: *security awareness*) и *безбедносне културе* која је спонтано прихваћена у организацији.

У оквиру овог поглавља дали смо појмовно одређење банака и њихову класификацију, као и осврт на Народну банку Србије као централне банке Републике Србије и главног регулатора ове области код нас и доносиоца докумената који се у ужем смислу односе на област заштите информација у банкама и финансијским институцијама.

Приказали смо неке банкарске пословне функције које су од значаја за функционисање система заштите информација, као што су пословна функција за контролу усклађености банке (енгл: *Compliance*) и унутрашња ревизија (енгл: *Internal Audit*), чиме смо показали да је безбедност пословна функција која се односи на функционисање целокупне организације, али и да безбедност зависи од функционисања других пословних функција у оквиру њихових пословних надлежности.

Банкарско пословање посвећује посебну пажњу ризицима и у том смислу се издвајају по значају: ризик ликвидности, кредитни ризик, каматни ризик, девизни ризик, и оперативни ризик – који привлачи нашу пажњу јер се односи непосредно на наш предмет истраживања.

Оперативни ризик је ризик могућности настанка негативних ефеката на финансијски резултат и капитал банке *услед пропуста у раду запослених, неодговарајућих унутрашњих процедура и процеса, неадекватног управљања информационим и другим системима, као и услед непредвидивих екстерних догађаја*.[432]

[430] *Ibid*, стр. 290.
[431] *Ibid*
[432] Џелетовић, М., Живковић, А., Бојовић, П., *op.cit.*, стр. 138. – 141.

Закон о банкама[433] уређује оснивање, пословање и организацију бананка, начин управљања банкама, као и контролу, реструктуирање и престанак рада банака, а у вези са предметом истраживања истакли смо да Члан 9б одређује тајне податке степеновано кроз категорије: „СТРОГО ПОВЕРЉИВО“, „ПОВЕРЉИВО“ или „ИНТЕРНО.

Управљње ризицима је одређено у Члану 28, где се експлицитно наводи да банка идентификује, мери и процењује ризике којима је изложена у свом пословању и управља тим ризицима, а Члан 29 препознаје оперативне ризике, укључујући правни ризик, као и ризик неодговарајућег управљања информационим и другим технологијама значајним за пословање банке.

Банкарска тајна је пословна тајна, регулисано је одељком о тајности података (Одељак 4). Банкарском тајном сматрају се (Члан 46):

4) подаци који су познати банци а односе се на личне податке, финансијско стање и трансакције, као и на власништво или пословне везе клијената те или друге банке;
5) подаци о стању и промету на индивидуалним депозитним рачунима;
6) други подаци до којих банка дође у пословању с клијентима.

Можда нејвећу важност за предмет истраживања представља *Одлука о минималним стандардима управљања информационим системом финансијске институције*. [434]

Чланом 5 је предвиђена обавеза за финансијксе институције да у складу са стратегијом пословања, као и с природом, обимом и сложеношћу пословања, *донесе стратегију развоја информационог система.*

Члан 16, који одређује обавезу *израде политике безбедности информационог система*, као унутрашњег општег акта којим се успоставља оквир за управљање безбедношћу тог система.

Управни одбор банке, односно надлежни орган финансијске институције, дужан је да донесе план континуитета пословања (енгл: *Business Continuity Plan*) и план опоравка активности у случају катастрофа (енгл: *Disaster Recovery Plan*) (Члан 26). Актом је одређен садржај ових докумената, укључујући обавезу формирања резервне локације за опоравак информационог система (резервни рачунарски центар), као и обавеза да се најмање једном годишње тестирају ови планови, а да се документовани резултати тестирања доставе надлежном органу.

Финансијска институција је дужна да обезбеди адекватно, континуирано стручно оспособљавање и обучавање запослених за коришћење информационих система и очување његове безбедности и функционалности (Члан 39).

[433] Закон о банкама, Службени гласник РС, бр. 107/2005, 91/2010 и 14/2015
[434] „Службени гласник РС“, бр. 23/2013, 113/2013, 2/2017 и 88/2019

Одлуком о управљању ризицима банке, Народна банка Србије прописује ближе услове и начин идентификације, мерења и процене ризика којима је банка изложена у свом пословању, осим ризика усклађености пословања.[435]

Банка је дужна да успостави такву унутрашњу организацију, односно организациону структуру којом ће активности управљања ризицима (енгл: *middle office*) и активности подршке (енгл: *back office*) функционално и организационо одвојити од преузимања ризика (енгл: *frong office*), с јасно утврђеном поделом послова и дужности запослених којом се спречава сукоб интереса (Члан 9).

Члан 17 налаже банкама да усвоје и примењују *стратегију развоја информационог система* и *политику информационог система*.

Одлука предвиђа да редовно, а најмање једном годишње, банка спроводи *стрес тестирање* на нивоу појединачно материјално значајних ризика којима је изложена (Члан 19а).

У вези са оперативним ризицима, банка је дужна да идентификује и процени догађаје и изворе због који могу настати губици у вези са оперативним ризицима, узимајући у обзир све значајне унутрашње и спољне факторе (Члан 65).
Ради обезбеђивања континуитета пословања управни одбор банке је дужан да усвоји план континуитета пословања (енгл: *Business Continuity Plan – BCP* план), као и план опоравка активности у случају катастрофа (енгл: *Disaster Recovery Plan – DRP* план), Члан 68.

Члан 69 прецизира да је банка ради спровођења континуитета пословања дужна да:

1) уврди кључне пословне активности (укључујући и оне које је поверила трећим лицима), ресурсе и системе потребне за обављање пословних процеса, као и њихову међузависност и повезаност;
2) утврди критично време за поједине пословне процесе, односно период после ког је неопходно поново успоставити ове процесе;
3) процени ризике који могу довести до прекида континуитета пословања банке и утицати на финансијско стање и/или репутацију банке;
4) процени вероватноћу настанка и значаја утицаја претходно наведених ризика
5) усвоји стратегију опоравка у којој ће утврдити следеће основне циљеве које треба да оствати у случају прекида пословања:
   - приоритете опоравка;
   - прихватљив ниво активности;
   - прихватљив ниво ризика и технике за ублажавање идентификованих ризика;
   - време опоравка, односно период до поновног успостављања редовних пословних процеса, који би требали да буду краћи у односу на критично време.

[435] „Службени гласник РС, бр. 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 – др. одлука 1, 43/2013, 92/2013, 33/2015, 61/2015, 61/2016, 103/2016 и 119/2017

На нивоу међународне координације банкарских политика опште су прихваћена правила које је дао Базелски комитет.

Базелски споразум је више пута мењан и допуњиван, а данас постоје: Базелски споразуми I, II и III, где нашу пажњу, полазећи од предмета истраживања, посебно привлачи Базел II, будући да он третира оперативни ризик, а претходно смо видели његов значај на област заштите информација у банкама и финансијским институцијама

Базел II се састоји из три стуба:[436]

1) стуб 1 дефинише минималне капиталне захтеве за кредитни, тржишни и оперативни ризик, уз могућност коришћења софистицираних модела и техника за њихово израчунавање;
2) стуб 2 учвршчује везу између оптималних капиталних захтева и врсте и степена ризика којима је банка изложена у свом пословању, уводећи процес интерне процене адекватности капитала (ICAAP) и јачајући процес супервизије;
3) стуб 3 употпуњује везу између стуба I и стуба II, истичући значај тржишне дисциплине увођењем минималних захтева за објављивање информација банака.

На основу Базел II НБС је донела следећа акта (објављена у „Службеном гласнику РС“, бр 45/2011 и 46/2011):[437]

- Одлука о адекватности капитала банке;
- Одлука о управљању ризицима банке;
- Одллука о објављивању података и информација банке;
- Одлука о контроли банкарске групе на консолидованој основи, и
- Одлука о извштавању и извештавању о адекватности капитала банке.

Од посебне важности за наш предмет истраживања, јесте истицање *значаја подизања свести запослених и културе понашања* у односу на изложеност оперативним ризицима, од стране Базелског комитета, као једног од приоритета у управљању оперативним ризицима. Постигнути успех у управљању ризицима директно зависи од начина на који се разуме и осећа процес управљања, јер су оперативни ризици уједно и ризици културе професионалног понашања свих запослених. Степен развијености културе понашања наспрам изложености оперативним ризицима, манифестује се као мања или већа осетљивост запослених на ове ризике, што прати и одговарајући степен могућих губитака. Чести су случајеви да се запослени суочавају са оперативним ризицима, а да тога нису ни свесни.[438]

Мишљења смо да је посебан допринос нашег истраживања у приказивању *резилијентности информационих система у банкама и финансијским институцијама*, јер је реч о савременом концепту у остваривању заштите информација у банкама. Традиционална процена ризика

[436] Доступно на: https://www.nbs.rs/internet/latinica/55/55_2/55_2_3/index.html
[437] Доступно на: https://www.nbs.rs/internet/latinica/55/55_2/55_2_3/o_propisima_bazel_II.pdf
[438] Совиљ, Р., Стојковић-Златановић, С., *op.cit.,* стр. 7.

подразумева сагледавање проблемске области кроз односе претњи, рањивости и последица које ће наступити, и у том смислу кибернетска безбедност постаје ограничена јер су потребни приступи за решавање претњи и рањивости који су примењиви (и ефиксни) у околностима сложених и међусобно повезаних система, одакле је тешко извести процену ризика која ће предвидети каскадне ефекте који би се могли догодити.[439]

Непредвидивост, екстремна несигурност и брзи развој потенцијала сајбер претње стварају ситуацију у којој је процена ризика све више неспособна да пружи адекватне одговоре који се односе на сајбер безбедност великих система, а посебно критичних инфрастуктура. Једина одговарајућа одбрана, наводе Линков и Кот, била би одвајање сајбер система од интернета, на исти начин на који биолошки системи развијају имунитет од инфекција и других напада, одакле се и сајбер системи морају прилагодити на сличан начин.[440]

Cyber Resilience, је предвиђање и прилагођавање променама у окружењу, задржавање и брзи опоравак од сајбер инцидента, наводи Сајбер лексикону који је издао Одбор за финансијску стабилност (енгл: *Financial Stability Board – FSB*).[441]

У раду смо представили документ о сајбер резилијентности финансијске тржишне инфраструктуре, издат од стране Банке за међународнано поравнања (БИС) и Међународне комисије за хартије од вредности (ИОСЦО), на основу чега смо приредили преглед садржаја компоненти и категорија сајбер резилијентности, што може помоћи будућа истраживања на овом пољу, а такође може користити и практичарима у банкама који раде на пословима заштите информација.

Издвојили смо као важно да се сајбер резилијентност у банкама и финансијским институцијама подразумева да заштита мора да обухвата информатичке ресурсе, али и заштиту људи и процеса; да се савремени концепт заштите обухвата и мере нетехничке природе, а посебно да у том смислу обухвата знања која долазе из менаџерских наука о управљању, планирању, организационој култури, едукацији запослених и сл.; и – да савремени концепт заштите информација обухвата и неке традиционалне области безбедности, као што су физичко-техничка заштита, безбедносне провере, безбедносне истраге и друго.

Ради будућих истраживања области заштите информација у банкама и финансијским институцијама, ми смо у овом поглављу упутили и на другу међународну нормативу која се односи на ову област.

---

[439] Linkov, I., Kott, A., *op.cit.*, стр. 6.

[440] *Ibid*

[441] ФСБ је тело које су основали шефови фржава и влада Г 20, у циљу промоције реформе међународне финансијске регулације и надзора. Доступно на: https://www.fsb.org/2018/07/cyber-lexicon-consultative-document/

У оквиру приказа међународних стандарда који се односе на заштиту информација дали смо приказ фамилије стандарда из серије ISO 27000, будући да они чине оквир за управљање заштитом информација (енгл: *Information Security Management System – ISMS*). Посебно, анализирали смо стандард ISO/IEC 27002, будући да он обухвата, између осталог, и организовање заштите информација у организацијама и законску усклађеност, одакле се односи на организационо и нормативно уређење заштите информација.Такође, упутили смо и на друге стандарде који се могу користити у заштити информација, као што су: *COBIT*, серију стандарда које је издао *NIST*, специфичпне стандарде као што су *PCI DSS* и Уредба Европског парламента о заштити појединаца у вези са обрадом личних података и слободном кретању таквих података (енгл: *General Data Protection Regulation – GDPR*).

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

1. Појам информационе безбедносне културе

У досадашњем истраживању више пута смо се дотакли појмова као што су безбедносна култура, информациона безбедносна кулутра, свест запослених о безбедности, организационо учење, организациона структура и друго.

Прегледом референтних научних радова који се односе на заштиту информација у банкама и другим финансијским институцијама, такође смо утврдили да су ови појови неодвојиви у изучавању овог феномена.

Заштита информација се бави људима, процесима и технологијом (Алнатир, 2012)[442].

Поред улоге технологије кључну улогу у култури информационе безбедности има улога менаџмента. Они заједно са запосленима утичу на вредности које су некада видљиве, а некада не. Прихватљив модел за развој културе заштите информација је само када у организацји постоје одговарајућа знања из ове области и када постоје одговарајуће активности запослених (Алвафаз, 2011)[443].

Друштвено-организациног приступ у управљању безбедности информационих система, између осталог, подразумева да су концепти поверења, културе и комуникације блиски и међусобно повезани, али и да то нису увек међусобно зависне променљиве. Безбедносна култура у организацији може бити јака, али ниво поверења низак, иако поверење олакшава успостављање снажне културе (Коскокас, 2004)[444].

[442] Alnatheer, M. A.: *Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia*, PhD Thesis, Faculty of Science and Technology, Queensland University of Technology, Brisbane, Queensland, Australia, 2012.

[443] Alfawaz, S.M.: *Information security management: A case study of information security culture*, Faculty of Science and Technology, Queensland University of Technology, 2011.

[444] Koskokas, I.V.: *A Socio-Organizational Approach to Information Systems Security Management in the Context of Internet Banking*, A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing at St. John's Brunel University, London, UK, 2004.

Безбедност постаје друштвени проблем, у којем се јављају нове методе угрожавања, одакле ће се банке у будућности бавити одређеном групом проблема међу којима су и питања одговорности менаџмента, као и питања одговорности запослених (Биркланд, 2015)[445].

Нормативни оквир је од значаја за заштиту информација, јер утиче на свест о безбедности (енгл: *security awareness*) – Бота, 2011.[446]

Недостатак безбедносне културе је уочљив и на индивидуалном и на организацином нивоу (Путник, 2012)[447].

Свака организација има јединствену културу, која утиче на брзину промена. Да би се промена усталила, неопходно је да је подстичу и прихватају сви запослени и на свим нивоима организаије. Промена (у безбедносној култури), неће се укоренити уколико је не прихвати послодовство, или уколико управа не верује у њену вредност, што је нарочито специфично у традиционалним хијерархијским организацијама (Станаревић, 2012)[448].

Подизање свести о информационој безбедности (енгл: *Information Secrurity Awareness – ISA*) могуће је организовати преко организационе културе. Када у организацији постоји безбедносна култура, аспекти информационе безбедности се реализују као природни рутински приступ од стране запослених (Андерсон, Густавсон, и Валден, 2008)[449].

Безбедност информација је вишедимензионална дисциплина и све димензије се морају узети у обзир да би се осигурало безбедно окружење. Према објављеној литератури и на основу разговора са стручњацима за заштиту информација, могу се утврдити неке димензије заштите информација, као што су: корпоративно управљање, организациона димензија, етичка димензија, улога људи, димензија свести и др. (Солмс и Солмс, 2004)[450].

Полазећи од стандарда ISO 17799, едукација корисника за заштиту информација је један од кључних фактора у остваривању заштите информација. У том смислу значајан је развој безбедносне свести (енгл: *security awareness*), односно једна од кључних активности је увођење програма о безбедносној свести у заштити информација, где је суштина у

---

[445] Birkeland, S.: *E-Banking security and organisational changes*, PhD dissertation, University of Liverpool, 2015.

[446] Lee Botha, C.: *A Gap Analysis to Compare Best Practice Recommendations and Legal Requirements when raising Information Security Awareness amongst Home Users of Online Banking,* Submitted in accordance with the requirements for the degree of Master of Science in the subject Information Systems, University of South Africa, 2011.

[447] Путник, Н.: *Кибер ратовање – нови облик савремених друштревних конфликата,* докторски рад, Факултет безбедности, Универзитет у Београду, Београд, Република Србија, 2012.

[448] Станаревић, С.: *Концепт безбедносне културе и претпостаке његовог развоја,* докторски рад, Факултет безбедности, Универзитет у Београду, Београд, Србија, 2012.

[449] Andersson, D., Gustavsson, M., Waldén, A.: *How a bank organization handles robberies – a question of crisis management,* Jonkoping International Business scool, Jonkoping University, Sweden, 2008.

[450] Solms, V.B., Solms, V.R.: *The 10 deadly sins of information security management,* Computers & Security, 2004.

едукацији корисника о њиховим појединачним улогама које они имају у остваривању овог система. Приступ оваквој едукацији треба базирати на образовним принципима заснованим на остваривању циљева тренинга (енгл: *outcomes-based education – OBE*), јер се овде не припремају запослени за даљи ниво формалног образовања, већ се оспособљавају за постигунуће конкретног циља – одговарајући ниво свести о информационој безбедности (Никерк, 2005)[451].

Никерк у остваривању подизања свети запослених о информациној безбедности види следеће важне полазишне тачке:

- заштита информација зависи од људи, а тренутни програми не придају довољно пажње теоријама понашања;
- неговање организационе субкултуре безбедности информација је неопходно у организацији, полазећи од теоријски добро проученог концепта промене корпоративне културе.

Постојеће обуке за подизање свести о безбедности углавном су техничке природе, а та чињеница и не чуди јер су безбедносне политике углавном исте такве, а то је опет из разлога што се менаџери који се баве заштитом информација претежно ослањају на смернице, стандарде, и друге документе који су углавном техничке природе, а које они обилато користе у креирању докумената за своју организацију. Корпоративне политике заштите информација састављају менаџери који имају мало знања о писању безбедносних политика (о контексту безбедности, наша је примедба), па излаз проналазе у ослањању на комерцијално доступне изворе као што је интернет, где их чекају чек листе (енгл: *checklist*), стандардизоване (технички профилисане) смернице и др. Истраживање *Ernst & Young's* из 2008. године говори да чак 70% анкетираних организација користи стандардизоване смернице, а очекивања су да ће тај тренд наставити са растом. Проблем са оваквом ситуацијом је што изостаје флексибилност за прилагођавање пословном систему за који се документи и програми подизања свести о безбедности праве, а посебно што изостаје социјални аспект безбедности (Харис, 2010)[452].

Домаћи аутори, поред до сада наведених, износе став да информациона безбедност подразумева сложене процесе који обухватају различите аспекте коришћења и заштите информационих технологија. Пре свега, потребно је дефинисати одговорности за све учеснике, јер је фактор „човек" најосетљивије место у свакој безбедносној шеми. Људи са

---

[451] Niekerk, J.F.: *Establishing and information security culture in organizations: an outcomes based education approach*, Dissertation submitted in fulfillment of the requirements for the degree Magister Technologiae in Information Technology, Faculty of Engineering, Nelson Mandela Metropolitan University, University in Port Elizabeth, South Africa, 2005.

[452] Harris, A. M.: *The shaping of manager's security objectives through information security awareness training*, PhD dissertation, Virginia Commonwealth University, 2010.

својим понашањем могу да пониште и најбољу заштиту: злонамеран запослени, непажљиви запослени, запослени који нису свесни политике и важности безбедности и др. Први корак у креирању уређеног система безбедности треба започети изградњом културе друштва у контексту рада и информацино безбедносном културом.[453]

Реч култура је латинског порекла, а значи обрађивање, неговање. Слично значење има и реч цивилизација која је такође латинског порекла а значи оплемењивање, углађивање. Према Оксфордском речнику култура се дефинише као: идеје, обичаји и друштвена понашања одређеног народа или групе људи. У литератури се могу пронаћи различита објашњења и схватања културе, као на пример аутора Палисписа, према следећем:

- култура представља дизајн или рецепте за живот – међусовно повезаних мрежа, норми и улога. Она обухвата моделе размишљања, осећања и деловања који се обично могу наћи у друштву и укључује све што је човек стекао као члан тог друштва;
- култура је дакле:
  i. карактеристичан производ људске интеракције;
  ii. сложено друштвено наслеђе које се преноси кроз друштво;
  iii. састоји се од експлицитних прихватљивих образаца за испуњавање билошких и друштвених потреба, а понашање се стицало и преносило симболима, који представљају карактеристична достигнућа људских група. Битно језгро културе чине традиционалне идеје и њихове промовисане вредности;
  iv. кумулативна, јер се преноси са генерације за генерацију у датом друштву;
  v. чиста је и апстракција;
  vi. људима пружа смисао јер је симбол квалитета;
  vii. научена је од сваке особе, као основа која детерминише њену личност, и
  viii. зависи од дужине континуираног функсионисања друштва, али је незвисна од било које специфичне групе.
- срце културе налази се у проналску и употреби алата, а пре свега у способности људи да уче из групе којој припадају. Значај и утицај културе на људе, као и све већа потреба за њиховом безбедношћу, довели су до нове научне дисциплине – безбедносне културе. Од ње се очекује да код људи подигне свест на прихватљив ниво, а тиме и промену њихових устаљених понашања.

Под безбедносном културом може се подразумевати безбедносна активност која изражава спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима. Такође, безбедносна култура огледа се у препознавању опасности, реаговању на њих избегавањем опасности, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати у сачувати

[453] Миловановић, З., Радовановић, Р.: *Информацино-безбедносна култура – императив савременог друштва*, журнал за криминалистику и право БНП, Криминалистичкко-полицијска академија, Београд, 2015. година, стр. 47. – 48.

угрожене вредности. Безбедносна култура треба да помогне корисницма да разумеју ризик и треба да их научи адекватним одговорима.[454]

Према мишљењу Стајића и сарадника, безбедносна култура представља скуп усвојених ставова, знања, вештина и правила из области безбедности, испољених као понашање и процес, о потреби, начинима и средствима заштите личних, друштвених и међународних вредности од свих извора, облика и носилаца угрожавања, без обзира на место или њихово време испољавања. Безбедносна култура је у тесној вези са нашим васпитањем, вредносима и вредносним системима које подржавамо.[455]

Миловановић и Радовановић наводе да се на основу свега наведеног могу констатовати три главна елемента која заједно чине безбедносну културу: технологија, политика (правила) и корисници.

Исти аутори су мишљења да свест о безбедности представља слабо дефинисану област, јер не постоји опште прихваћена дефиниција која описује свест корисника о информационој безбедности – што значи и да не постоји заједничко разумевање свести о безбедности. Свест се може посматрати и као компетентност људи да ураде праву ствар. Свест о безбедности помаже људима да схвате важност едукације и тренинга везаних за безбедност. Знати нешто није исто као и променити понашање и стечене навике. Циљ тренинга је практична примена новостечених знања и промена понашања при коришћењу нових технологија, а знање о нечему је само један корак ка промени тог понашања.[456]

Миловановићи и Радовановнић преносе ставове Чие (енгл: *Chia*) и сарадника, да не постоји јасна и општеприхваћена дефиниција информационе безбедносне културе, а да су неке од најчешће коришћених:[457]

- Дилон, одређује безбедносну културу као свеукупност људских особина, као што су понашање, ставови и вредности, које доприносе заштити свих врста информација у датој организацији;
- Солмс, позива на стварање информацино-безбедносне културе у оквиру организације, тако што ће се сваком запосленом усадити информационо-безбедносни аспект као рутина у вршењу свакодневног посла;
- Мертин и Елоф описују је као производе понашања запослених у вези са информацином безбедношћу, која током времена прераста у „начине на које се раде ствари";
- Шлајнгер и Тујфел одређују ифнормацино-безбедносну културу као све друштвено-културуолошке мере које подржавају активности техничких метода, тако да информациона безбедност постаје природан аспект дневних активности сваког запосленог;

[454] *Ibid*
[455] *Ibid*, стр. 49.
[456] *Ibid*, стр. 51.
[457] *Ibid*, стр. 52.

- Кизисто и сарадници, навдое да процес формирања безбедносне културе подразумеав укључивање скупа вредности свих заинтересованих страна. Они тврде да ако се обједине вредности свих чланова органиације, онда се обједињена култура може формирати за мање од неколико година, међутим, ако вредности у организацији нису обједињене, онда је тај период знатно дужи (ми би додали и неизвеснији);
- Гоу и сарадници дефинишу информационо-безбедносну културу као начин на који запослени и организација као целина раде ствари које се односе на информациону безбедност;
- Роер у књизи „Изградња безбедносне културе" истиче да она помаже и олакшава људима да користе информационе технологије на задовољавајући начин, без опасности и претњи.

Аутори наводе да информацино-безбедносну културу на сличан начин дефинишу и други истраживачи, па тако наводе: Кизиста и Илвонена (енгл: *T. Kuusisto, I. Ilvonen, 2003*), Врума и Солмса (енгл: *C. Vroom, R. Solms, 2004*) и Томсона и сараднике (енгл: *K. Thomson, R. Solms, L. Louw, 2006*), и сматрају да се може закључити да се нформационо.безбедносна култура у организацији манифестује кроз различите аспекте безбедости које се односе на: вредност, понашања, ставове, акције, активности менаџмента, као и физичко окружење.

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

Проблем одређења концепта информационе безбедносне културе је врло присутан у многим радовима, полазећи од значаја који она данас има, а што смо утрдили у досадашњем току истраживања – посебно у делу о нормативној уређености, где смо кроз најсавремени приступ изложен у делу о резилијентном приступу у остваривању заштите информација уочили колико се савремени концеп заштите информација базира на равномерном приступу техничких и нетехничких мера, као и проблему развоја свести запослених и развоју информационе безбедносне културе .

Тако је група аутора, у раду објављеном почетком 2020. године, покушала да утврди концепт културе информационе безбедности кроз сагледавање питања шта она сама представља у организацијама.[458]

У раду је анализиран досадашњи теоријски научни допринос, али су испитивани и стручни ставови професионалаца у индустрији безбедности о постављеном проблему истраживања.

[458] Veigaa, A., Astakhova, Lj. V., Bothac, A., Herelmanc, M.: *Defining organisational information security culture—Perspectives from academia and industry*, Computer & Security, Volume 92, May 2020. Доступно на: https://www.sciencedirect.com/science/article/pii/S0167404820300018?via%3Dihub

Индустријска перспектива културе информационе безбедности добијена је коришћењем квантитативних и квалитативих метода истраживања, уз употребу анкете, да би се онда анализа добијених резултата интегрисала у перпективу досадашње литературе – што сматрамо добром методологијом за будућа истраживања на пољу заштите информација и иначе, на пољу изучавања безбедносне проблематике.

Аутори наводе да упркос разноврсним дефиницијам и интерпретацијама културе безбедности информација, постоје низ заједничких аспеката, који се огледају у позивању на вредности и на понашање запослених.

Култура информационе безбедности обухвата мишљење, осећаје и свакодневне активности запослених (*Da Veiga and Eloff, 2010; Schlienger and Teufel, 2002; Van Niekerk and Von Solms, 2010).*

Посебна пажња посвећена је вредностима које усмеравају запослене у оцењивању понашања да ли је прихватљиво или неприхватљиво прилиом обраде информација *(Dhillon et al., 2016; Van Niekerk and Von Solms, 2010).*

Култура информационе безбедности фокусира се на социо-културе аспекте управљања инофрмацином безбедности *(Schlienger and Teufel 2002).*

На бази Шајнове (*Schein*,2009) дефиниције организационе културе, култура информационе безбедности је природни аспект у свакодневним активностима сваког запосленог *(Schlienger and Teufel, 2002).*

Шајн је је дефинисао појам организационе културе као образац заједничких основних претпоставки на основу којих је група научила како да решава проблеме спољне адаптације и унутрашње интеграције, а формулисане су довољно добро да се могу сматрати вредним и као такве преносити новим члановима организације, као исправан начин перцепције, размишљања и осећања за исте проблеме.[459]

Накнадна истраживања културе информационе безбедности такође су укључивала концепт знања *(Helokunnas and Kuusisto, 2003; Van Niekerk and Von Solms, 2010).*

Остале дефиниције културе безбедности информација имале су свеобухватнији приступ, укључујући концепте перцепција, вредности, претпоставки и знања *(AlHogail and Mirza, 2014).*

Такође, неки аутори сматрају да је заштита информатичких добара организације циљ културе безбедности информација *(Alfawaz et al., 2010).*

Људи су истовремено и препрека и циљ у остваривању зашите информација *(A. da Veiga, L.V. Astakhova and A. Botha et al. 2020).*

Данас је све више аутора склоно да културу информационе безбедности сагледа из хумане перспективе, јер су људи критични ресурс у том смислу. Особа може да постане или објекат

[459] С. Станаревић, *op.cit*., стр. 243. – 244.

или предмет социјалног инжењеринга. Из тих разлога, у посматраном раду је уведен концепт културе информационе и психолошке сигурности, дефинисан као начин организовања и развоја животне активности, у којем је субјекат информацијске интеракције препознат као субјекат информационе и психолошке сигурности *(Astakhova, 2011).*

У организацији различите организационе целине могу да имају различите супкултуре информационе безбедности (*Da Veiga and Martins, 2017).* Ако супкултура информационе безбедности не доприноси заштити информација, она се онда може назвати контракултуром, која је деструктивна ка заштити података *(Astakhova, 2010).* Контракултуре се морају идентификовати да би се спроводиле усмерене акције које би их ускладиле са доминантном културом безбедности информација, Астахова је увела концепт културног капитала, користећи консолидацију знања, понашања и вештина, што организацији даје одређени друштвени статус и положај у друштву *(Cole, 2019).*

Аутори су у свом истраживању дефиниције културе безбедности информација користили специјализовани софтвер, на основу чега су дали преглед најважнијих 16 радова, са освртом да ли је у раду дата формална дефиниција или опис културе безбедности информација.[460]

На описани начин аутори су дошли до листе најучесталијих термина који се користе за дефинисање или описивање културе безбедности информација, које су груписали и дали према следећем (Табела број 11: *Садржај информационе безбедносне културе*):

- спољашњи фактори: национална култура (на пр.: различито разумевање приватности), нормативно уређење (закони, подзаконска акта и др.), економски фактори (кризе, степен корупције и сл.), социо-културни фактори и технички и технолошки фактори;
- унутрашњи фактори: организациони, менаџмент фактори, људски фактори и међусобно поверење запослених, послодавца и клијената.

Аутори су, на основу свог истраживања понудили дефиницију информационе безбедносне културе:

Информациона безбедносна култура дата је у контексту понашања људи, које се односи на заштиту информација које организација обрађује, кроз поштовање одговарајућих политика и процедура и разумевања како да се тако дефинисани захтеви спроводе на опрезан и пажљив начин, тако, да је то понашање уграђено у редовну комуникацију, свест, обуку и образовне иницијативе. Временом, такво понашање постаје део начина на који се размишља и на који се обављају пословни процеси, што постаје део претпоставки запослених, њихових вредности и веровања, као и део њихових знања и перцепције према заштити информација. Култура заштите информација је усмерена визијом вишњег менаџмента, заједно са подршком менаџмента и у складу са политиком безбедности информација и под утицајем унутрашњих и спољашњих фактора, и подржана од стране адекватног *IT* окружења, што је видљиво у производима (енгл: *artefacts*) организације (говор, технологија, производи,

[460] За потребе истраживања аутори су користили софтвер *Publish or Perish software*. Доступно на: https://harzing.com/resources/publish-or-perish

креације и сл.) и понашању запослених, стварајући тако окружење поверења са заинтересовним странама и успостављање интегритета.[461]

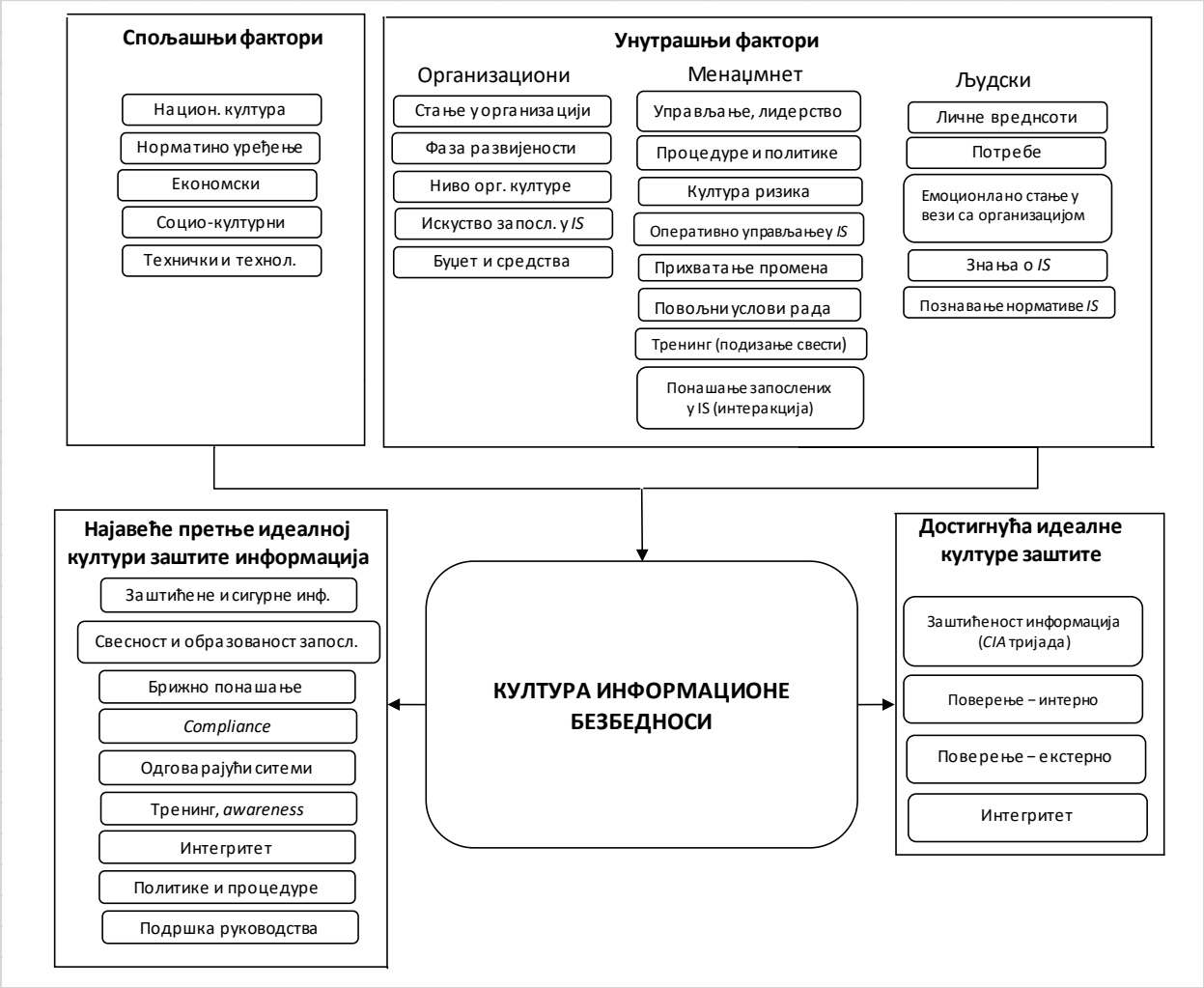
Табела број 11: ***Садржај информационе безбедносне културе***[462]

	ФАКТОРИ	ОПИС
СПОЉАШЊИ	Национална култура	
	Нормативно уређење	
	Економски фактори	
	Социо-културни фактори	
	Технички и технолошки фактори	
УНУТРАШЊИ ФАКТОРИ	Организациони фактори	Стање у организацији (стабилност, динамичност, пословне активности)
		Ниво развијености организације (енгл: *Stage of the life cycle*)
		Ниво организационе културе
		Искуство запослених у заштити информација
		Ресурси (буџет и средства)
	Менаџмент фактори	Управљање, лидерство
		Политике и процедуре у информационој безбедности
		Култура ризика у заштити информација
		Оперативно управљање у заштити информација (примена стандарда као што су *ISO 27001* или *Cobit)*
		Change management (прихватање промена)
		Стварање повољних услова рада (здовољство послом, контроле, мониторинг безбедности, награде, казне и др.)
		Тренинг, обука, подизање свести
		Понашање запослених у сфери безбедности (интеракција)
	Људски фактори	Личне вредности (одговорност, интегритет, поверење, етичност, мотивација и др.)
		Потребе (лично незадовољство може бити окидач за намерне инциденте и сл.)
		Емоционлано стање запосленог у вези са радом у организацији
		Знања о заштити информација
		Познавање политика заштите информација
	Међусобно поверење запослених, послодавца, корисника услуга	Поверење према радном окружењу
		Повређе клијената у организацију

[461] Veigaa, A., Astakhova, Lj. V., Bothac, A., Herelmanc, M., *op.cit.*, стр. 19.
[462] Прилагођено према: Veigaa, A., Astakhova, Lj. V., Bothac, A. и други, *Op. cit.*, стр. 9. – 11.

Полазећи од предмета истраживања нашег рада, посебну вредност посматраног научног рада видимо у представљању модела информационе безбедносне културе у организацији (Схема број 21: *Модел информационе безбедности културе у организацији*).

Схема број 21: ***Модел информационе безбедности културе у организацији***[463]



Теорија се до сада бавила и утврђивањем ширег појма – организацине културе, где информациона безбедносна култура свакако представља подсистем, или њен посебан део, у мери у којој је и безбедност данас постала део опште културе. Нама је ова веза важна да би у даљем раду дали нека појашњења основних појмова који се у теорији користе за објашњење појмова организације и организационе културе, будући да се општа правила из

[463] *Ibid*, стр. 20.

ове области односе и на информациону безбедносну културу, као подсистема организационе културе.

У раду о димензијама организационе културе, неки аутори полазе од разумевања овог појма као широког термина који се користи за дефинисање особености и карактера организације, који укључује елементе као што су основне вредности и веровања менаџмента и запослених, њихове етичности и међусобна правила понашања.[464]

Такође, организациона култура се може дефинисати као начин како се одређене ствари раде у предузећу.[465]

Организациона култура је скуп неформалних веровања и понашања који постоје у организацији и које је организација прихватила као свој начин обављања процеса. Док се формална страна односи на писане изјаве и начин функционисања према организационој структури, неформална страна се односи на начин обављања посла, односно начин на који се запослени понашају једни према другима и колико су спремни да размењују идеје и информације. Дефиниција организационе културе попут „начина на који се обављају одређене ствари", „ритуала у компанији", „климе у организацији", „основних вредности" и друго, нису довољно прецизне и посматрају само поједине аспекте концепта организационе културе. За свеобухватно дефинисање концепта важно је схватити да се организациона култура може посматрати само кроз своје манифестације у вербалним комуникацијама и формама понашања чланова посматране групе.[466]

У циљу што прецизнијег дефинисања организационе културе, неопходно је посматрати шта одређена група дели или има заједничко.[467]

Потребно је узети у обзир чињеницу да култура егзистира у различитим слојевима организације тако да је, да би се њоме управљало, потребно управљати и оним најдубљим слојевима организације, који су углавном невидљиви.[468]

У посматраном научном раду аутори су дали преглед најзначајнијих емпиријских истраживања у области организационе културе (укупно 17 аутора који су објављивали о

[464] Спасојевић Бркић, В. К. *et al.*: *Димензије организационе културе у мултинационалним предузећима*, часопис Техника, број 69, Београд, 2019. године, позивају се на дело: *Корпоративна култура и организациона структура*, Цвијановић, Ј., Лазић, М., Настасић, А., Економски институт, Београд, 2006. година. Доступно на: https://scindeks-clanci.ceon.rs/data/pdf/0040-2176/2019/0040-21761902279S.pdf

[465] *Ibid*, аутори се позивају на извор: R. Burman, A. J. Evans, *Target zero: A culture of safety*, Defence Aviation Safety Centre Journal, pp. 22-27

[466] *Ibid*

[467] *Ibid*, стр. 280., аутори се позивају на извор: E. Schein, *Organizational culture and leadership*, Second Edition, Jossey-Bass, San Francisco, 1997.

[468] *Ibid*, аутори се позивају на извор: E. Schein, *The corporate culture survival guide*, , Jossey-Bass, San Francisco, 2009.

организационој култури у периоду од 1916. до 2007. године), и том приликом су закључили да се у теорији углавном говори о следећим њеним димензијама, и то:[469]

- преузимање ризика у организацији;
- структура организације;
- брзина реаговања организације;
- начин комуницирања у организацији;
- усредсређеност организације на циљеве, односно резултате;
- степен формализације у организацији:
- систем награђивања у оорганизацији;
- механизам контроле у организацији;
- однос организације према конфликту;
- знање и компетентност запослених;
- прогрес и развој запослених, и
- примарна оријентација организације.

Емпиријским истраживањем аутора, обухваћена су предузећа познате мултинационалне компаније, заједно са њиховим добављачима и партнерима, који су распоређени на шест континената (Северна Америка, Јужна Америка, Европа, Азија, Аустралија и Африка), и том приликом су закључили да постоје следеће димензије организационе културе у мултинационалним предузећима:

- предузећа настоје да применом одговарајућих алата структуирано управљају ризиком;
- предузећа не поседују сложене организационе структуре са много управљачких нивоа, великим административним апаратима и високим нивоима хијерархије и бирократије;
- у погледу брзине реаговања организације услед поремећајних фактора (унутрашњих и спољашних) предузећа су подељена;
- комуникација у организацији је кључна и важно је да информације увек буду доступне;
- циљеви и задаци предузећа су јасно мерљиви. Такође, обезбеђено је континуирано праћење њихове реализације у циљу благовременог предузимања корективних акција;
- предузећа се ослањају на добро дефинисана правила и процедуре која чине висок ниво формализације у овим организационим системима;
- прдузећа имају развијен систем награђивања запослених који се успешно примењује;
- предузећа не поседују стриктан механизам контроле, укључујући и управљачки апарат;
- у циљу успешног управљања конфликтима у оквиру своје организације, предузећа примењују одговарајуће стратегије за управљање конфликтом;

[469] *Ibid.*, стр. 282.

- с обзиром да су знање и компетентност запослених најважнији за ефикасно пословање, предузећа редовно инвестирају у обуку и професионални развој;
- могућност за развој личних компетенција и могућност унапређења додатно мотивише запослене;
- предузећа нису искључиво окренута ка тржишту или ка својим интерним процесима, већ оба аспекта третирају као подједнако важна;
- најбитније димензије организационе културе, према компанијама које су обухваћене истраживањем, су: управљање ризиком, развијена комуникација у организацији, постављање мерљивих циљев и задатака, поседовање развијеног формализованог система процедура и њихова употреба, примена система награђивања, решавање конфликата у организацији, улагање у знање и компетентност запослених и њихово редовно унапређивање и развитак.

Иако у истраживању није наведено експлицитно која индустрија је била предмет истраживања, сматрамо да су наведени закључци корисни и за сагледавање феномена организационе културе у банкама и финансијским институцијама – посебно јер аутори наводе опште димензије организационе културе, према досадашњим теоријским радовима, како смо претходно дали, што очекујемо да има своје импликације и на информациону безбедносну културу, уважавајући ниво општости од општег ка појединачном (организациона култура – безбедносна организациона култура – информациона безбедносна култура), што може бити тема будућих научних радова.

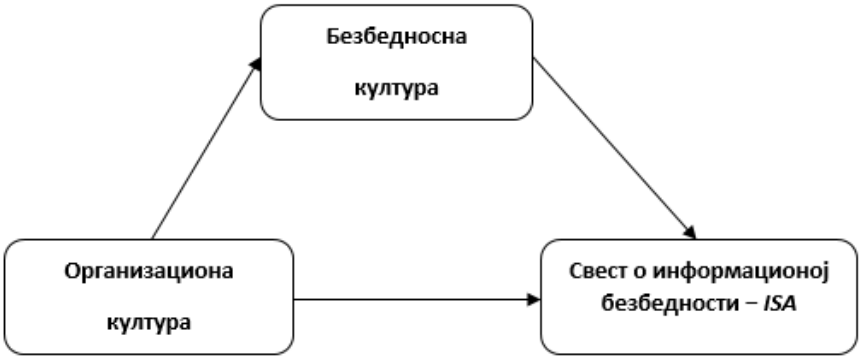
Wileya, McCormac и Чалић, урадили су 2020. године, истраживање о односу између културе и информационе свести, у којем су на основу спроведене анкете закључили да *постоји значајан позитиван однос између организационе културе, културе безбедности и свести о информационој безбедности.*[470]

Они наводе да је истраживањем пронађена снажна позитивна линеарна веза између организационе културе и културе безбедности. Како се организациона култура повећавала, тако се повећавала и безбедносна култура. Ова веза, како наводе аутори, подржана је претходним истраживањима и у складу је са теоријским аргументима који сугеришу да је безбедносна култура подкомпонента организационе културе (*A. Veiga, N. Martins*, 2015.; A. Nasir *et al*, 2019.).[471]

[470] Wileya, A., McCormac, A., Čalić, D.: *More than individual: Examing the relationchip berween culture and information security Awareness*, Computer & Security, Volume 88, january 2020, доступно на: https://www.sciencedirect.com/science/article/pii/S0167404819301841

[471] Veiga, A., Martins, N.: *Information security culture and information protection culture: A validated assessment instument*, Computer Law & Security Review, Volume 31, 2015., pages 243.-256., доступно на: https://www.sciencedirect.com/science/article/abs/pii/S0267364915000060; A. Nasir *et al*, An analysis on the dimensions of information security culture concept: A review, Journal of Information Security and Applications, Volume 44, February 2019, pages 12-22. Доступно на: https://www.sciencedirect.com/science/article/abs/pii/S2214212617306828

Схема број 22: ***Однос организационе културе, безбедносне културе и свести о информационој безбедности (енгл: Information Security Awareness – ISA)***[472]



Такође, што је од значаја за наше истраживање, пронађена је значајна позитивна линеарна веза између безбедносне културе и свести о информационој безбедности (*ISA*), у складу са (K. Parsons *et al*, 2014).[473] Како се култура безбедности повећавала, тако је расла и свест о информационој безбедности (Схема број 22: *Однос организационе културе, безбедносне културе и свести о информационој безбедности (енгл: Information Security Awareness – ISA*).

Посебно издвајамо налаз да је су у суштини испитаници из организација са јачом безбедносном културом имали већу вероватноћу да имају бољи *ISA.*

Аутори наводе да иако постоји веза између организацационе културе и свести о информационој безбедности, она је под јаким утицајем безбедносне културе. Овај налаз сугерише да *без обзира на организациону културу, јака култура безбедности може боље да предвиђа раст свести о информационој безбедности*, што последично доводи до закључка да је можда боље фокусирати се на развој безбедносне културе, ако је предмет дискусије раст свести о информационој безбедности, него на развој организационе културе.[474]

У раду је показан и утицај извесних демографских променљивих, где се дошло до закључка да је свест о информационој безбедности била већа како се старост испитаника повећавала – и то је почело да се примећује код група које су биле старије од 40 година старости. Значајне разлике нису утврђене између мушких и женских испитаника.

Можемо да закључимо да је теорија потврдила нашу претпоставку да постоји значајна веза између организационе културе, безбедносне културе и свести о информационој

[472] Прирећено према: Wileya, A., McCormac, A., Čalić, D., *op.cit.*, стр. 5.

[473] Parsons, K.: *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q),* Computers & Security, Volume 42, 2014, pg. 165-176, доступно на: https://www.sciencedirect.com/science/article/pii/S016740481300179X

[474] A. Wileya, A. McCormac, D. Čalić, *Ibid*, стр. 5.

безбедности, услед чега ћемо, као и на основу до сада истраженог у поглављима о информационој безбедности и нормативног уређења заштите информација, посебно изнетог о информационој резилијентности, у даљим разматрањима сагледати основне теоријске поставке из којих произилази одређење организационе културе, односно ближе ћемо сагледати области организационог понашања и организационих промена – или, организације као научне области науке о менаџменту.

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

У досадашњем истраживању више пута смо истакли чињеницу да савремено друштво, између осталог, одликује значај информација као и развој технологија које прате поступање са њима, одакле се јавила потреба заштите овог стратешког ресурса.

Ради остваривања својих интереса, људи се удружују у различите форме организација, од предузећа до међународних заједница, одакле се јавила потреба за изучавањем организација, као још једне особине савременог друштва.

Организације се проучавају у оквирима менаџмента јер се организовање врши у циљу управљања предузећем или неким другим обликом организације. Из тог разлога, организовање се сматра једном од фаза процеса управљања. Менаџмент се дефинише као процес планирања, организовања, вођења и контроле напора чланова организације и осталих ресурса ради остваривања циљева организације. Менаџмент као процес има четири фазе, и то:[475]

- *планирање*, обухвата процес постављања циљева организације и одређивање подесног тока акције да би се ти циљеви реализовали;
- ***организовање***, је процес диференцијације и интеграције чланова организације како би се на најбољи начин искористили њени ресурси и остварили постављени циљеви;
- ***вођење***, представља процес мотивисања, усмеравања и утицаја на чланове организације да обаве постављене задатке;
- *контрола*, је процес утврђивања да ли се рад организације подудара са планираним и предузимања корективних акција уколико то није случај.

Област организације обухвата фазе организовања и вођења, где се *проучава структуирање рада чланова организације кроз ефикасан дизајн, као и узроци и облици понашања људи у*

[475] Петковић, М., Јанићијевић, Н., Богићевић, Б.: *Организација*, Економски факултет, Београд, 2002. године, стр. 15.

њима – одакле се у нашем истраживању наметнула потреба разумевања ове области менаџмента.

Разлози за овакав приступ у нашем истраживању су вишеструки, а огледају се првенствено у чињеници да смо предмет истраживања ближе одредили кроз организационо и нормативно уређење заштите информација у банкама и финансијским институцијама.

У организационом смислу, дали смо преглед могућег организовања послова заштите информација у банкама и финансијским институцијама, у поглављу о информационој бебедности, којом приликмо смо дали коментаре на предности и недостатке појединих модела организовања послова, односно где смо сагледали импликације које дају поједина решења на перформансе ове пословне функције.

У нормативном смислу, сагледали смо нормативне оквире које карактеришу амбијент организовања заштите информација у предметним организацијма, где смо уочили да се савремени концепт организовања ових послова, сајбер резилијентност, у великој мери односи на посматрање и утицање на понашање људи у организацији – будући да је теорија сагласна да су људи истовремено и носиоци заштите информација, али и најслабија карика у остваривању овог система, јер својим понашањем, активностима и односом, представљају и извор угрожавања ових стратешких ресурса.

Коначно, у оквиру овог поглавља, показали смо да постоји значајна веза између организационе културе, безбедносне културе и свести запослених о информационој безбедности – што је представљало још један аргумент да области организације, како смо претходно навели, посветимо потребну пажњу.

3.1. Области истраживања организације као научне области

Теорија менаџмента је сагласна да се у истраживању организације издвајају као посебне целине три области, и то:

- организациона теорија и дизајн (енгл: *Organizational Theory and Design – OT*);
- организационо понашање људи у организацији (енгл: *Organizational Behavior – OB*);
- организационе промене и развој (енгл: *Organizational Change and Development – OD*).

Организациона теорија и дизајн има за свој предмет проучавања структуралне, формалне или „тврде“ елементе организације. Основни области проучавања су организациона структура и системи, са следећим темама истраживања:

- подела рада,
- дистрибуција ауторитета доношења одлука;

- груписање јединица
- број хијерархијских нивоа;
- распон контроле руководилаца;
- координација;

Циљ истраживања *ОТ*-а је моделирање структуре и система организације како би се у одређеним типичним ситуацијама применили одговарајући модели. У њеном развоју највећи допринос су дали истраживачи техничког профила образовања, па је услед овога утицај технике, а данас можемо рећи утицај информационе технологије, врло јак (у области структуре). Организациона теорија и дизајн су добро истражене области, услед чега је ретка појава нових радова.[476]

Организационо понашање (*ОВ*) за свој предмет изучавања има следеће области:[477]

- изучавање понашања појединаца и група у организацијама;
- разумевање, објашњавање и предвиђање понашања појединаца и група унутар организација;
- могућност бољег и ефикаснијег управљања понашањем појединца;
- начин настанка корпоративне културе и њен утицај на понашање појединца и обрнуто.

Организационо понашање захтева интердисциплинарни приступ, будући да је наслоњена на друге друштвене науке, као што су: социологија, социологија културе, психологија, економија и антропологија.

У области нашег истраживања, она се односи на истраживање понашања појединаца и група у области заштите информација, пре свега у погледу развоја безбедносне културе и свести о безбедности информација (енгл: *security awareness*).

Два су основна задатка истраживача у организацином понашању: објаснити понашање људи и окрити начин на који се на њега може утицати. Основне теме истраживања у овој области су најчешће подељене на три нивоа људског понашања и то индивидуални, групни и организациони ниво.

Индивидуално понашање се истражује кроз перцепцију и учење, мотивају, вредности и ставове. То су варијабле које у значајној мери објашњавају понашање појединаца у организацији. Варијабле које објашњавају понашање два или више појединаца (групе) су: вођство, групе и тимови, конфликти и моћ. На организационом нивоу понашање људи се истражује анализом организационе културе, комуникација и организационог учења.[478]

[476] *Ibid.*
[477] Џамић, В.: *Организационо понашање и корпоративна култура*, Универзитет Сингидунум, Београд, 2016. године, стр. 2.
[478] Петковић, М., Јанићијевић, Н., Богићевић, Б., op.cit., стр. 16.

Данас је ово област организације у којој се врши највише истраживања. За разлику од организационе теорије и дизајна, у овој области су највећи допринос дали истраживачи хунманистичког профила образовања: психолози, социолози, социјални психолози, антрополози.[479]

Организационе промене и развој (*OD*) је најмлађа област организације и почиње да се развија од средине шездесетих година прошлог века, са појавом концепта организационог развоја.

Предмет истраживања ове области је промена организације, као и на који начин изводити те промене. Теме интересовања су узроци који доводе до промена, садржај организационих промена као и сам процес промена. Циљ је открити правила за успешно и ефикасно извођење промена у организацијама тако да се оне обаве са најмањим трошковима и највећим користима. Највећи допринос у развоју ове гране организације су дали консултанти, наводећи своја практична искуства у овој области.[480]

Мишљења смо да је корисно за будућа истраживања заштите информација дати преглед научних области организације и њиховог односа са појединим областима заштите информација (Табела број 12: *Преглед области организације и однос према областима заштите информација*).

.**Табела број 12:** ***Преглед области организације и однос према областима заштите информација***

Област организације	Теме истраживања	Однос са заштитом информација (енгл: *information security – IS*)
Организациона теорија и дизајн	– подела рада, – дистрибуција ауторитета доношења одлука; – груписање јединица – број хијерархијских нивоа; – распон контроле руководилаца; – координација;	Место *IS* у организацији
Организационо понашање	– изучавање понашања појединаца и група у организацијама; – разумевање, објашњавање и предвиђање понашања појединаца и група унутар организација; – могућност бољег и ефикаснијег управљања понашањем појединца; – начин настанка корпоративне културе и њен утицај на понашање појединца и обрнуто.	Понашање запослених према *IS* (енгл: *security awareness*)
Организационе промене и развој	– узроци који доводе до промена; – садржај организационих промена; – процес промена	Промене *IS* у организацији

[479] *Ibid.*
[480] *Ibid*, стр. 17.

У досадашњем истраживању нашег рада, својим значајем истакле су се теме које се односе на организационо понашање, односно на информациону безбедносну културу, одакле ћемо размотрити допринос организационе теорије овој области истраживања.

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

Проучавање организационог понашања повезано је са очекиваним понашањем појединца у организацији.[481]

Кондалкар, попут већине других аутора, наводи да је тешко пронаћи две особе које ће се понашати на идентичан начин у одређеној ситуацији, одакле, наше је мишљење, извире важност људског фактора и у области заштите информација, будући да очекујемо од запослених да се понашају на одређени начин према информатичким ресурсима, а посебно очекујемо да је њихово понашање стандардизовано у условима нарушавања безбедности информација.

Организационо понашање представља подручје организације које проучава понашање људи у организацијама, од нивоа појединца, преко радних група, до организације као целине.[482]

Руководиоци у организацији треба да буду у стању да објасне, предвиде, процене и модификују људско понашање, што у великој мери зависи од њиховог знања, вештина, и искуства у руковођењу, у различитим ситуацијама. Да би се људско понашање предвидело потребно је предузети одређене превентивне активности. Систем вредности, емоционална интелигенција, организациона култура, организациони дизајн, важни су фактори који утичу на људско понашање, којом приликом *организациона култура може модификовати понашање појединца*. Област организационог понашања обухвата следећа питања:[483]

- утицај личних особина на перформансе;
- мотивацију;
- лидерство;
- стварање ефикасних тимова и група;
- проучавање различитих организационих структура;
- појединачно понашање, став, учење;
- перцепцију;
- дизајн и развој ефикасне организације;
- дизајн послова;

[481] Kondalkar, V. G.: *Organizational Behavior*, New age international limited, New Delhi, 2015., стр. 3., доступно на: https://www.iibms.org/wp-content/uploads/2015/05/Organizational-Behaviour.pdf
[482] Петковић, М., Јанићијевић, Н., Богићевић, Б., *op.cit.*, стр. 239.
[483] Kondalkar, V. G., *Ibid,* стр. 3. - 4.

- утицај културе на организационо понашање;
- управљање променама;
- сукоб и управање стресом;
- организациони развој;
- организациона култура;
- групно понашање, моћ и политка;
- дизајн послова;
- проучавање емоција.

Понашање људи може бити прописано или научено. Прописано понашање је одређено писаним правилима, а *научено понашање оно које је временом прихваћено као неписана норма понашања у датој ситуацији*.[484]

На овој идеји, наше је мишљење, базиран је читав концепт развоја свести о информационој безбедности (енгл: *security awareness*), будући да су очекивања, у идеалној ситуацији, да запослени примењује научено на тренинзима о информационој безбедности као саставни део свог понашања (дакле не само због тога што организација од њега очекује да, на пример, не отвара линкове из мејлова које је добио са сумњиве адресе, већ да такав *mail* пријави организационом делу који је задужен за заштиту информација) – а не због евентуалне казне која може да уследи уколико запослени буде „ухваћен" у прекршају.

Организационо понашање је интердисциплинарна научна област организације, која се ослања на фундаменталне науке о човеку, његовом понашању и односима, које се називају бихејвиористичким наукама (психологија, социологија, социјална психологија, антропологија), с једне стране, и на емпиријска истраживања са друге стране.[485]

Психологија истражује, мери и објашњава промене у понашању живих бића. Тежиште је на проучавању понашања јединке. У савременој организацији изучава се: учење, перцепција, личност, лидерство, потребе и мотивација, задовољство послом, процес одлучивања, стрес на послу итд.

Социологија, за разлику од психологије, пажњу усмерава на проучавање социјалних система у којим су појединци организовани у групе. У организацији проучава се група и групни процеси у организацији, организациона култура, радни тимови, утицај технологије, организационог дизајна, комуникација, моћи, конфликата и др.

Социјална психологија интегрише претходно наведене концепте (психологије и социологије), а њен допринос се огледа у области мерења, разумевања и промене ставова запослених, комуникацијских модела, утица група и тимова на перформансе организације и задовољство запослених, процеса доношења одлука итд.

[484] Петковић, М., Јанићијевић, Н., Богићевић, Б., *op.cit.*, стр. 239.
[485] *Ibid*, стр. 243.

Антропологија се бави изучавањем традиције, обичаја и других националних обележја, што доприноси изучавању различитих култура, разумевању културних разлика, разлика у ставовима и понашању запослених у различитим земљама и различитим организацијама.

Домаћи аутори препознају три приступа у одређивању фактора организационог понашања: менталистички, бихејвиористички и приступ друштвеног учења, где се под менталистичким приступа понашање људи објашњава одговором организма на унутрашње подстицаје и подразумева да је понашање људи њихова индивидуална ствар, занемарујући при томе његове интеракције са околином – док бихејвиористички приступ истражује објективно понашање и посматра човека као отворен систем, који успоставља интеракције са околијном. Приступ сугерише да се понашање може предвидети и контролисати помоћу управљања променљивом околином.[486]

Нашу пажњу привлачи приступ друштвеног учења, јер понашање човека објашњава као функцију личних карактеристика и интеракција са средином у којој човек ради, односно са организацином средином.

„Човек долази у организацију са личним карактеристикама, које су одређене генетским факторима, искуством и учењем. У организационој средини личне карактеристике се испољавају у начину понашања које је вођено ставовима, индивидуалним системом вредности и веровања, способностима и личним циљевима. С друге стране, организациони фактори, као што су природа делатности, карактеристике технологије, дизајн организације, стил лидерства и друго, директно утичу на понашање појединца у организацији. Смисао приступа друштвеног учења, на којем се заснива модел организационог понашања јесте у могућностима предвиђања и променама понашања, ради прилагођавања.”[487]

Ови наводи представљају још једно место где видимо могућности развоја свести о информациној безбедности, као облика друштвеног учења у организацији, будући да се на овај начин може предвидети и променити понашање запослених према заштити информација – одакле ставови запослених према информациној безбедности нису коначна категорија, већ се они мењају са временом (и у складу са активностима организације на изградњи безбедносне културе), и на њих је могуће утицати.

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

Основни модел организационог понашања, како наводе Петковић, Јанићијевић и Богићевић, укључује три нивоа анализе, велики број независних варијабли (енгл: *input*), које утичу на понашање запослених, као и зависних варијабли (енгл: *output*) које се јављају као

[486] *Ibid*, стр. 246. - 247.
[487] *Ibid*

индивидуалне, групе и организационе перформансе (Схема број 23: *Модел организационог понашања*).[488]

Зависне варијабле су аутпути којима се тежи, односно то је оно што менаџмент жели да постигне, и што је обично дефинисано документима, као што су: план, стратегија, визија и др.

Независне променљиве представљају инпуте који утичу на понашање запослених и на које менаџери имају различит степен утицаја на појединим нивоима. *На индивидуалном нивоу* за понашање су пресудне *личне карактеристике појединца* и ту су могућности утицаја менаџера релативно мале. Како се људи понашају различито када су у групи, у односу на то када су сами, то повећава могућност утицања на понашање од стране менаџера у смислу њиховог утицаја на понашање, путем развоја и промена групних односа и групних процеса. Из ових разлога *групни ниво је најзначајнији у организацији, јер менаџери могу да постигну високе перформансе* развијајући добре међуљудске односе и радећи на развоју људи. *На организационом нивоу*, кључне варијабле преко којих менаџери утичу на понашање запослених су: карактеристике делатности и технологије, *организациона култура*, дизајн организације и дизајн посла (ниво специјализације, појава монотоније, досаде и стреса).

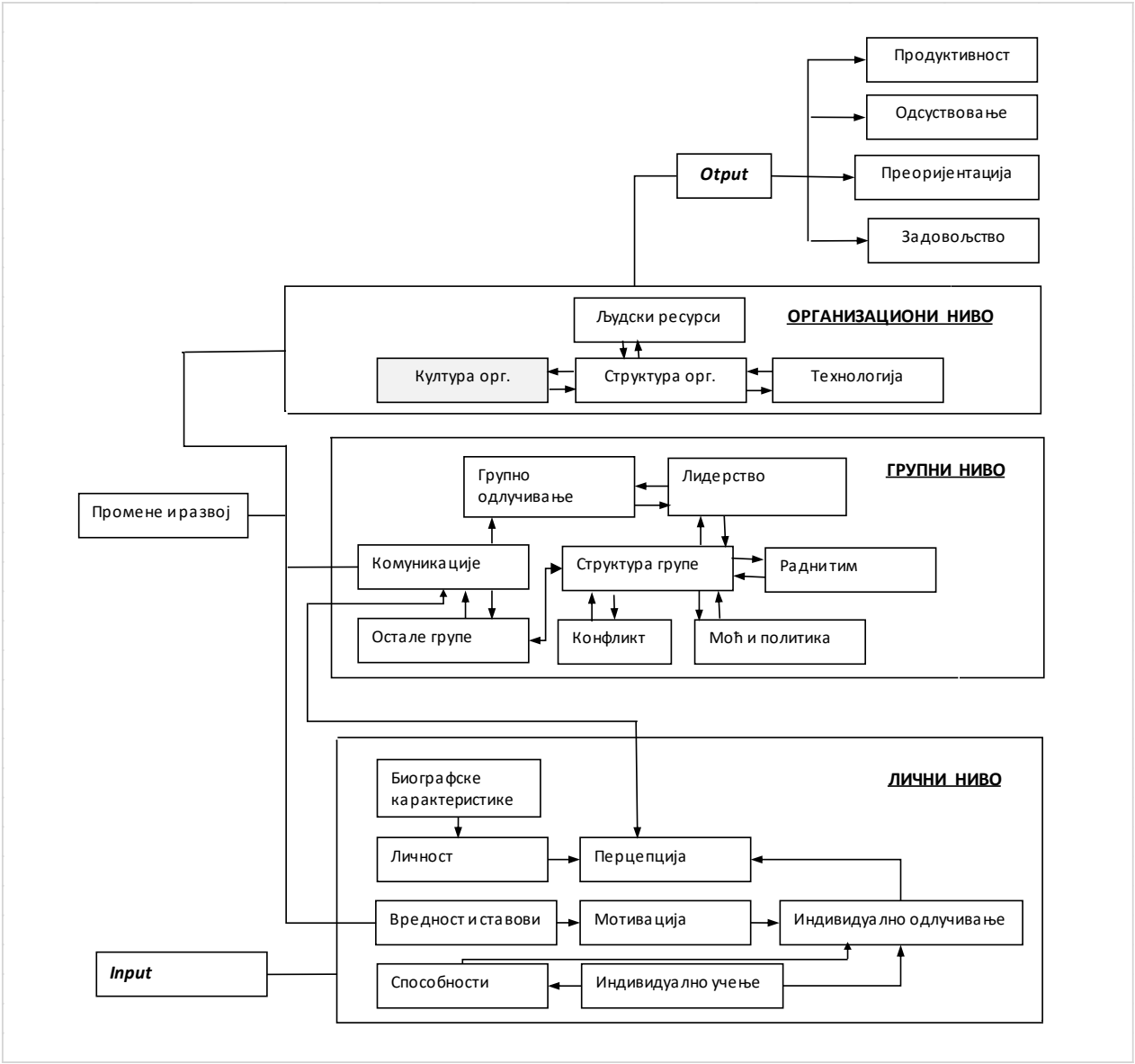
У досадашњем истраживању ми смо у неколико наврата приказали научна истраживања која се односе на културу информационе безбедности, као део организационе културе, што смо обрадили у поглављу референтних научних радова.

Суштина свега до сада изнетог је у методолошком моделу који се може користити за истраживања о заштити информација, где можемо да закључимо да се манипулисањем независних променљивих може утицати на жељене аутпуте, односно – да утицањем на факторе који утичу на ниво организационе културе, дакле и безбедносне, односно културе заштите информација у организацији, можемо утицати на крајњи резултат, као што је ниво заштите информација у организацији.

Тако би, у вези са предметом нашег истраживања, будући научни радови могли да се баве испитивањем различите врсте независних променљивих, као што су утицај места пословне функције заштите информација у организацији на остваривање информационе безбедности, утицај образовног профила руководилаца заштите информација на перцепцију запослених о безбедности, повезаност тренинга из информационе безбедности са ефикасношћу система за заштиту информација у организацији и друго.

[488] *Ibid*, стр. 247. - 248.

Схема број 23: ***Модел организационог понашања***[489]



[489] *Ibid*

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

Станаревић наводи да је најпознатији теоретичар који се бавио организационом културом, Едгар Шајн, развио концепт и дефинисао појам организационе културе као „образац заједничких основних претпоставки на основу којих је група научила како да решава проблеме спољне адаптације и унутрашње интеграције, а формулисане су довољно добро да се могу сматрати вредним и као такве преносити новим члановима организације, као исправан начин перцепције, размишљања и осећања за исте проблеме."[490]

Ауторка наводи и дефиницију где се органзациона култура дефинише на основу интеракција запослених на радном месту и условљена је њиховим животним искуством, снагама и слабостима, образовањем и васпитањем. Она се такође заснива на заједничким ставовима, веровањима, обичајима, експлицитним или имплицитним уговорима, и писаним и неписаним правилима на основу којих се организација развија током времена и који су функционисали веома успешно да би се сматрали важећим. Други назив за организациону културу који се сусреће у литератури јесте корпоративна култура и може се рећи да се манифестује у следећем:

1) начину на који организација обавља свој посао, третира своје запослене, клијенте, као и ширу заједницу;
2) мери у којој су аутономија и слобода дозвољене у доношењу одлука, развијању нових идеја и личном изражавању;
3) начину на који моћ и проток информација пролазе кроз хијерархију;
4) снази запослених и обавезама према колективним циљевима.[491]

Станаревић наводи да постоје многи заједнички елементи у великим организацијама било које земље, али да је она особена за сваку организацију и најтеже се мења. Обликовање специфичне културе организације зависи од спољашњег окружења (економски, социјални фактори, научно-технолошки развој, и др.) и од унутрашњих фактора, који обухватају мисију, стратегију и технологију организације. Руководство организације игра велику улогу у дефинисању организационе културе кроз своје поступке и лидерство, јер је задужено за обликовање филозофије организације, која одражава циљеве, вредности, уверења, идеје које се најбоље оваплоћују у личности оснивача и председника (или генералног менаџера). Свака оргранизација има јединствену културу, која покреће облик, степен и брзину промена. Да би се иновација усталила, неопходно је да је подстичу и прихватају сви запослени и на свим нивоима. Промена се неће укоренити уколико је не прихвате високи лидери.[492]

---

[490] Станаревић, С.: *Концепт безбедносне културе и претпоставке његовог развоја*, докторски рад, Факултет безбедности, Београд, 2012. година, стр. 243. - 246.
[491] *Ibid*
[492] *Ibid*

Неки савремени радови о организационој култури наводе да се она може сагледати кроз четири нивоа.[493] Прво, свака култура је јединствена. Чак и ако различите организације имају исти циљ, оне до њега могу доћи различитим путевима. Друго, организациона култура даје јасне смернице за проналажење потенцијалних запослених, будући да се на тај начин траже сарадници који ће се добро уклопити у организацију, и на тај начин ће и они сами добро напредовати, а са њима и организација. Треће, организационе културе су флуидне и оне са са временом мењају, одакле их треба узгајати и неговати. Ако се мисија компаније мења, организациона култура мора такође да се промени. Четврто, организације могу преко организационе културе да утичу на свој спољашњи идентите, а пример за то су данас најуспешније компаније.[494]

У истом раду је дат податак, на основу студије која је рађена у Америци, а где је праћен развој 207 великих компанија, из 22 индустрије и у периоду од 11 година, да су организације које су водиле рачуна о организационој култури значајно повећале цене својих акција (у студији се наводи да је то чак девет пута), у односу на организације које то нису радиле (оне су у периоду посматрања повећале цене акција за дупло). Нето приход је за ове прве повећан за седам пута, а компаније које нису водиле рачуна о развоју своје организационе културе, имале су минимално, једва приметно повећање.[495]

Јанићијевић је дифинисао организациону културу као систем претпоставки, веровања, вредности и норми понашања које су чланови једне организације развили и усвојили кроз заједничко исксутво, који су манифестовани кроз симболе и који усмеравају њихово мишљење и понашање.[496]

Гонзалес је дефинисао корпоративну културу као скуп значења и симбола које људи користе за организовање идеја, интерпретације искуства, доношење одлука и вођење акција.[497]

Домаћи аутори наводе да је за разумевање појма организационе културе потребно разумети следеће:[498]

Организациону културу чине *елементи когнитивих стуктура* чланова организације, као што су: претпосавке, веровања, вредности итд. Поред ових елемената организациону

---

493 Morcos, M.: *Organisational culture: definitions and trends*, 2018. Доступно на: https://www.researchgate.net/publication/329140215_ORGANISATIONAL_CULTURE_DEFINITIONS_AND_TRENDS

494 *Ibid*, аутор се позива на чланак: Y. Weiner, *99 Totally Serious Ways To Create A Great Work Culture*, 2018. Достпуно на: https://medium.com/thrive-global/99-totally-serious-ways-to-create-a-great-work-culture-e7d093bdad23

495 *Ibid*, аутор се позива на чланак: Xiaoming, C., Junchen, H.: *A literature Review on Organization Culture and Corporate Performance*, International Journal of Bussiness Administration, Vol. 3, No. 2, 2012., Доступно на: http://www.sciedu.ca/journal/index.php/ijba/article/view/863

496 Петковић, М., Јанићијевић, Н., Богићевић, Б., *op.cit.*, стр. 391. - 394.

497 Џамић, В.: *Организационо понашање и корпоративна култура*, Универзитет Сингидунум, Београд, 2015. година, стр. 73.

498 Петковић, М., Јанићијевић, Н., Богићевић, Б., *Ibid*

културу чине и *симболички елементи*, као што су: језик, материјални симболи, обрасци понашања и др.

Важна карактеристика културе је да је то социјална категорија, у смислу да постоји само у оквиру социјалних група, као што су организације, професије и слично.

Организациона култура усмерава или чак одређује свест и понашање људи. Сви чланови организације на приближно исти начин интерпретирају и разумеју појаве у свету око себе, одакле се усмерава и одређује и њихово свакодневно понашање.

Организациона култура настаје кроз процес социјалне интеракције и комуницирањем чланова организације.

Утицај организационе културе на успех организације видели смо и у представљању студије (енгл: *Weiner*) где је праћен успех предузећа у периоду од једанаест година, а поред тога домаћи аутори сматрају да је карактерише и следеће:[499]

- организациона култура је значајан фактор у доношењу стратешких одлука, будући да се оне доносе под утицајем полазних претпоставки и веровања које доносиоци одлука имају;
- организациона култура је значајна за пословање предузећа као детерминанта његове способности да се променама прилагођава окружењу, што је стални процес. Треба напоменути да снажна организациона култура може и да блокира промене, што би био негативан ефекат на способност прилагођавања предузећа;
- организациона култура представља механизам координације у предузећу, јер када запослени полазе од истих претпоставки и вредности, онда се лакше разумеју и координација је ефикаснија;
- организациона култура може бити ефикасан механизам контроле понашања запослених, а на тај начин је могуће постићи и контролу мишљења и осећања запослених;
- организациона култура смањује конфликте у организацији, јер су чест узрок конфликата управо различити оквири од којих људи полазе у разумевању света око себе. Када запослени полазе од различитих претпоставки, вредности и веровања о свету око себе, конфликт је неминован;
- организациона култура је добар мотиватор, јер подстиче поистовећивање чланова организације са њоме. На тај начин људи задовољавају своју потребу за припадањем, уколико је реч о снажној култури.

У области безбедносне културе, наведене карактеристике се испољавају у свим наведеним елементима, а посебно у вези са прилагођавањем условима окружења и интерној координацији и контроли. Политике (стратегије) заштите информација које доноси пословодство, треба да су усаглашене са организационом културом (дакле и са безбедносном културом чије је неодвојиви део и култура заштите информација), што

[499] *Ibid*

повећава ефикасност таквих политика и олакшава процес контроле, будући да запослени, у случају развијене организационе културе, прокламоване вредности прихватају као логичан наставак личних веровања, ставова и очекивања, а не доживљавају их као наметнута правила против којих се треба борити, јер нису „природна“ за то окружење.

4.1. Садржај организационе културе у контексту унапређења заштите информација

Претходно смо изнели ставове домаћих аутора да се садржај организационе културе може класификовати на когнитивну и симболичку компоненту организационе културе.

Когнитивне елементе организационе културе чине: веровања, вредности, очекивања, претпоставке, етика, осећања, значења, неформална правила, начин мишљења, поглед на свет.

Базичне претпоставке представаљају најдубљу компоненту когнитивног садржаја културе и имају дескриптивну функцију, како наводе домаћи аутори, позивајучи се на Шајна.[500] Оне систематизују и генерализују основна људска сазнања и искуство људи о томе како свет око њих функционише. У поређењу са веровањима, претпоставке су много дубље, а знање и искуство које систематизују су општег и апстрактног карактера, па у том смислу имају већи утицај на понашање људи. Са животним искуством оне се потискују у подсвест, одакле их је тешко открити и мењати.

Веровања, слично као и базичне претпоставке, могу да буду потиснуте у подсвест, одакле делују по аутоматизму, а настају када се временом одређене вредности у пракси покажу успешним. Оно што је на почетку ефикасно решење, прелази преко стања коме треба тежити и правила како треба реаговати у свим сличним случајевима у реално стање ствари. На тај начин *треба* постаје *јесте*. У остваривању заштите информација, јака организациона култура развија вредности код запослених, да, на пример, информација представља стратешки ресурс организације и да заштита зависи од свесности појединца и од његових поступака. Веровање да осетљиве податке не делимо непоузданим изворима треба да је саставни део и приватног понашања запосленог у личној комуникацији. У слабој организационој култури (безбедносној култури), запослени ће уобичајено на друштвеним мрежама делити информације о својој организацији, процесима које сами обављају, којом приликом се готово по правилу преувеличава важност пословних процеса које појединац обавља за организацију, што злонамерним особама опет даје довољно информација и мотива за планирање напада. У банкама, то би могло да буде хвалисање службеника трезора како свакодневно преко својих руку броји огромне своте новца, а да се то посебно интензивира пред викенд или празник, када у банци остаје још већа сума новца од уобичајено велике. Пример би могао да буде и објављивање на друштвеним мрежама

[500] *Ibid,* стр. 394. - 399.

фотографије са радног места, где запослени поткрепљује своје тврдње колико је његов посао одговоран и колико његова организација зависи од њега.

Вредности представљају одређену врсту идеала којем појединац, организација или друштво треба да тежи и који треба да усмерава понашање и активности.[501]

Ставови представљају стабилан систем веровања појединца да се у некој ситуацији треба понашати на одређен начин. У остваривању заштите информација, то би могао да буде став запослених да пажљиво приступају дељењу информација са непознатним саговорником, чак и када се саговорник позива на ауторитет, којом приликом је потребно да запослени изврши додатне провере аутентичности саговорника и да о истом обавести своје радно окружење и непосредног руководиоца, ради заузимања става групе.

Норме понашања, представљају правила понашања у стандардизованим ситуацијама, којом приликом се подразумевају ситуације као што су начин међусобног обраћања запослених, обављање свакоднених активности које не морају да буду у вези са радним процесом (да ли се примају приватне посете или не, да ли се на паузе одлази организовано и под којим условима и друго), начин заказивања и одржавања пословних састанака и слично.

Симболички садржај организационе културе обухвата све оно у организацији што има неко значење за њене чланове, било материјалне или нематеријалне природе.

Језик као семантички симбол представља најзначајнији симбол културе и изражава знања и искуство припадника организације. У њему су садржана значења која чине културни садржај, услед чега се у свакој култури развија специфичан језик.

У поглављу о заштити информација, навели смо истраживање које је утврдило да од 800 прикупљених стручних речи и израза који се користе у банкарској индустрији у Републици Србији, чак половина има своје синониме на српском језику, али се и поред тога примењују изрази на страном (енглеском) језику.[502] На истом месту у нашем истраживању, дали смо допринос разумевању претежне употребе термина „сајбер безбедност" у односу на „информациону безбедност", што теоријски није основано, али представља праксу у свету индустије заштите информација – што у крајњем има своје импликације на хипотетички оквир нашег истраживања, где смо изнели претпоставку да заштита информација у банкама и финансијским институцијама запоставља нетехничке мере заштите.

Приче, представљају такође семантички симбол организационе културе. Свака организација има своје приче чија је улога да преносе организацији одговарајућу врсту поруке, која обично представља неко важно веровање, вредност или претпоставку која се жали установити или учврстити у организацији.[503] У области заштите информација, приче могу бити корисне у спровођењу тренинга, где се на одговарајућим примерима из живота

[501] *Ibid*
[502] Више о томе: Александар Ђ. Вулетић, *Контакти енглеског и српског језика у области банкарства и финансија*, докторска дисертација, Филолошки факултет, Универитет у Београду, Београд, 2013. године, доступно на: http://nardus.mpn.gov.rs/bitstream/handle/123456789/4044/Disertacija.pdf?sequence=1&isAllowed=y
[503] М. Петковић, Н. Јанићијевић, Б. Богићевић, *Ibid*

организације могу поткрепити ставови о некој области информационе безбедности. Тако, на пример, потребу закључавања радне станице приликом напуштања радног места, може поткрепити прича о злоупотреби радне станице од стране злонамерног колеге, која се заиста догодила у тој организацији и која је релативно свима већ позната. Приче се причају да би се претпоставке, вредности и веровања потврдили, али и пренели онима који за њих још не знају или их до тада нису прихватили. Митови представљају измишљене приче или непотврђена веровања, али могу имати исте функције као и приче.

Бихејвиористички симболи, као што су ритуали и церемоније, обухватају различите обрасце, моделе и устаљене начине понашања чланова организације. Ритуали су стилизоване активности које имају за циљ да изазову одређене ефекте, али и да пренесу одређејне културне вредности и веровања. Тако на пример, додела пригодног поклона поводом неког јубилеја који је запослени остварио, са одговарајућом свечаношћу, говором представника менаџмента, представља ритуал који велича вредност лојалности предузећу. Ритуали стварају границу између чланова организације који прихватају прокламоване културне вредности и оних који то не чине.[504]

Материјални симболи су највидљивији део организационе културе и обухватају материјалне објекте који имају за циљ да одразе одређена веровања и вредности чланова организације.[505] Пример би могла бити пракса држања отворених врата канцеларије надређеног руководиоца, где је порука да је он увек доступан за своје сараднике.

4.2. Класификација организационих култура и механизми унапређења заштите информација

Неки домаћи аутори се позивају на типологију култура коју су дали Харисон и касније Ханди (енгл: *Handy*), према којој постоје четири основан типа културе: култура моћи, култура улога, култура задатка и култура подршке.[506]

Култура моћи је заснована на њеној оријентацији ка лидеру, где у пракси могу истовремено постојати крајности где је то облик диктатуре и где у свом најбољем издању може да ствара слику породице. Избор моћи не мора да буде само контрола ресурса (као што су новац, информације и сл.), већ то може да буде и харизма лидера. Ова култура није бирократска, а у њој не постоји поштовање правила и процедура. У култури моћи комуницирање је врло интензивно и неформално. Главна предност ове културе је брзина реаговања, а недостатак је што све зависи само од једне особе – лидера. У оваквим организацијама влада ауторитаризам и сви способни менаџери обично одлазе у друге организције. Погодна је за мале и младе организације, у којима не доминира високообразовани кадар и за турболенте

[504] *Ibid*
[505] *Ibid*
[506] *Ibid*, стр. 400. - 402.

индустрије где је потребно брзо реаговање. Вероватно, наше је мишљење, најбољи пример за овакву индустрију је индустрија приватног обезбеђења код нас и у земљама окружења.

Култура улога је права бирократска култура, будући да у њој доминирају правила и процедуре. Са тог аспекта, погодна је као форма за развој заштите информација, уколико су испуњени и други потребни услови, као што је у првом реду безбедносна свест запослених. Оно што је у култури моћи лидер, то су овде правила и стандарди. У култури улога све се заснива на логици, разуму и рационалности. Заснива се на виђењу организације као уређеној социјалној структури, коју регулишу договорена правила и процедуре. Култура улога је деперсонализована, а моћ се стиче на основу хијерархијске позиције. Култура улога највише одговара људима који траже сигурност на послу, који воле предвидивост и избегавају промене и ризик. Најчешће се налази у великим бирократизованим организацијама као што је јавна управа и својим амбијентом одбија динамичне, предузетне људе.

Култура задатка је такав систем вредности и веровања у којем су највише вредности успех и постигнуће, одакле се некада тако и назива. Култура задатка почива на претпоставци да организација постоји да би решавала задатке. Људи се не цене према хијерархијској позицији већ према њиховој способности да допринесу реализацији задатка. У овој култури се цене карактеристике као што су самосталност појединца, флексибилност и прилагодљивост. Најподеснија је за релативно мале, специјализоване организације, као што су консултантске делатности, адвокатске канцеларије и сл. Основни недостатак је у претераној зависности од људи и њихових квалитета.

Култура подршке је тип културе који се у пракси најређе проналази. Почива на претпоставци да организација постоји да би омогућила њеним члановима да остваре своје индивидуалне циљеве и интересе, одакле је тешко веровати да би организација са оваквом културом могла да опстане на тржишту. Високо се цени индивидуална слобода и пружа се отпор сваком напору да се организационим правилима та слобода ограничи. Организације са оваквом културом су у сталној опасности од распада, а то се и догађа када њени чланови процене да је најбоље даље наступати индивидуално. Најчешће се налазе на факултетима и у истраживачким установама.

Банке и друге финансијске институције најчешће теже ка моделу културе улога, што је имајућу у виду наведено о овом облику организационе културе, повољан амбијент за развој заштите информација и уопште – за развој безбедносне културе. Такође, одавде извире и значај који има место послова безбедности у хијерархији организације.

4.3. Безбедносна култура као супкултура организације

Организације имају доминантну културу и своје супкултуре, које представљају специфичан систем претпоставки, вредности, веровања, норми и симбола које дели једна мања група запослених у организацији.[507]

У цитираном раду, као и у многим другим радовима које смо овом приликом истраживали, овај појам се пише као *субкултура,* што није правилно, будући да правопис налаже да се изврши једначење по звучности (дакле исправно је – супкултура).[508]

Супкултуре се могу посматрати по три основна правца: хоризонтално, вертикално и дијагонално.[509]

По вертикалној линији се могу разликовати супкултуре менаџера и запослених, односно супкултуре топ менаџметна и нижих организационих делова. Није редак случај да се вредности и веровања руководства организације значајно разликују од вредности и веровања осталих запослених. Овоме доприноси не само разлика у образовању, друштвеном положају или животном стандарду између менаџера и запослених, већ и различити проблеми са којима се они срећу у свакодневном раду, као и различите перспективе гледања на пословање. Некада ће вредности и веровања нижих руководилаца бити ближа њиховим сарадницима него топ менаџменту организације.

Хоризонтални правац диференцијације се често поклапа са професионалним супкултурама. Поделе рада и специјализације довеле су до диференцијације пословних функција, где оне могу да имају различите циљеве, различиту технологију рада, различити профил и ниво образовања запослених, различиту улогу у организацији, различите перспективе пословања, па и различите проблеме. Ове разлике у супкутурама представљају снажан извор проблема у области координације у организацији.[510]

Дијагонална диференцијација се одвија према различитим критеријумима: према професији и образовању, према социјалном пореклу и статусу, према специјалним интересовањима, хобијима и др. Такође, могуће је поредити разлике између система вредности и веровања старијих и млађих запослених.

Супкултуре се могу разликовати и на основу њиховог односа према доминантној култури организације, када се разликују: подржавајуће, оргогоналне и контракултуре.

---

[507] *Ibid*, стр. 402. - 403.

[508] Миљковић, Ј., Шрам (*Schram*), М.: *Организациона субкултура и образовање запослених*, часопис Андрагошке студије, Институт за педагогију и андрагогију, број 1, 2015. године, стр. 122., наводе да је термин субкултура распрострањен у српској научној јавности, па се користи и у њиховом раду. Правопис налаже да се изврши једначење по звучности (супкултура), од чега су свесно одустали. Доступно на: http://www.as.edu.rs/search?s=Organizaciona+subkultura+i+obrazovanje+zaposlenih&l=sr

[509] Петковић, М., Јанићијевић, Н., Богићевић, Б., *op.cit*., стр. 402.

[510] *Ibid*

Подржавајуће супкултуре садрже све вредности и веровања доминантне културе, али су оне снажније, једноставније и чистије.

Ортогоналне супкултуре садрже вредности и веровања која су независна од оних која чине садржај доминантних култура. Овде се прихвата доминантна култура, али се и развија систем додатних вредности и веровања која произилазе из специфичних интересовања.

Контракултура је супкултура која садржи потпуно другачије вредности, веровања и норме у односу на доминантну културу. Припадници ове супкултуре су „отпадници" од стране владајуће културе, али и представљају најчешће носиоце промена доминантне организационе културе, одакле је присуство контракултуре драгоцено у организацијама које су у кризи.

Примећујемо да је теоријски концепт односа доминантних култура и супкултура од значаја за наш предмет истраживања, будући да овај однос препознајемо у остваривању заштите информација у организацијама кроз дискусију о месту информационе безбедности и хејарарријској структури.

На више места у раду изнели смо запажање да често различите пословне фунцкије могу да имају различите пословне циљеве. Тако смо навели, да пословна функција IT-а има за циљ да своје пројекте реализује ефикасно, што је и очекивајуће јер целокупно пословање зависи од ове функционалности организације. Са друге стране, информациона безбедност захтева анализе и трага за логичним одговорима и на тај начин трага за пропустима у организацији. Како смо већ навели у разматрањима о моделу где је информациона безбедност смештена у пословну функцију IT-а, оно што за ову пословну функцију мора да се обави сада и одмах, за информациону безбедност не само да не мора да значи, већ је и очекивајуће да приоритет буде аналитичност, а не брзина.

Слично можемо да посматрамо и неке друге пословне функције у банкарском пословању. Оно што је важно за развој пословања и нове услуге, као што је на пример дигитализација банкарских сервиса у услуга, за безбедност може да буде критично уколико се поштују само захтеви ове пословне функције. Бизнис жели што отворенију услугу према клијентима, у смислу да им је она лако доступна (и у буквалном и у преносном смислу, и у смислу уласка клијената у простор банке без додатног задржавања на процедуре уласка, а и у смислу да се захтева што мање контрола и верификација идентитета корисника приликом обављања услуга електронског банкарства), док безбедност има за циљ да отворености према клијентима не представљају и додатне изворе угрожавања.

У смислу свега наведеног, сматрамо да основано можемо да говоримо у супкултури безбедности у организацијама, као и да различите групе у организацијама имају различита веровања и вредности према безбедности, односно према заштити информација, што је посебно изражено у хоризонталној диференцијацији култура, где смо видели да разлике у супкултурама представљају снажам извор проблема у области координације у организацији.

Диференција супкултура у организацији представља још један аргумент о значају свести о безбедности (енгл: *security awareness*), будући да се спровођењем обука може утицати на промену свести, односно на промену вредности и веровања унутар сваке супкултуре у организацији.

Посебан проблем за остваривање система заштите информација у организацијама, представљају контракултуре, одакле верујемо да у будућим истраживањима треба истраживати начине како политике информационе безбедности могу направити трансформације од контракултуре, до доминантне културе организације.

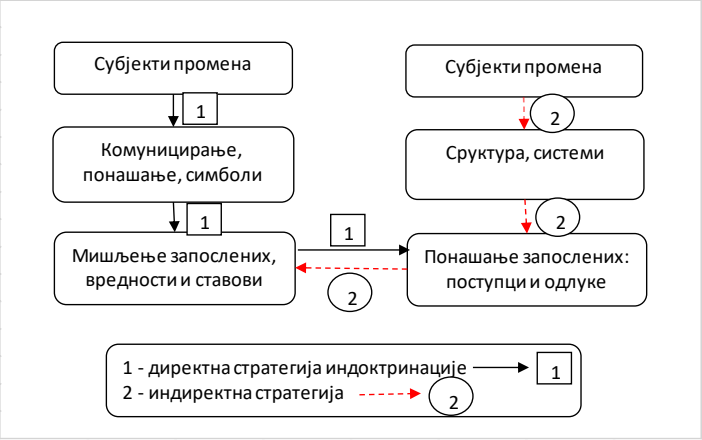
4.4. Могућности унапређења културе заштите информација кроз спровођење стратегије промене организационе културе

Јанићијевић наводи да организацона култура настаје као процес стварања заједничких претпоставки, веровања, вредности, норми и симбола и њиховог прихватања од свих или већине запослених и настаје у процесу групног (колективног) решавања проблема, кроз решавање проблема екстерне адаптације и интерне интеграције.[511]

Екстерна адаптација се односи на проналажење места организације у својој средини, а интерна интеграција обезбеђује складно функционисање и хармоничне међуљудске односе како би организација постала компактна социјална заједница.

Промена организационе културе подразумева два основна начина на који се може мењати корпоративна култура: директна стратегија и индиректна стратегија (Схема број 24: *Стратегије промене организационе културе*).

Схема број 24: *Стратегије промене организационе културе*[512]



[511] *Ibid*, стр. 403.
[512] *Ibid*, стр. 406.

Директна стратегија је стратегија индоктринације, и састоји се у директном утицају на ставове и вредности запослених из којих произилази промена понашања. Састоји се у томе да се запосленима шаљу директне поруке о томе какви су ставови о појединим питањима која чине корпоративну културу. Стратегија се базира на комуникацији са запосленима, одакле ефикасност стратегије зависи од ње. Три су основне групе средстава којима се реализује стратегија директне промене културе, и то:

- директно комуницирање са запосленима;
- невербално комуницирање (преноси се понашањем, или примером);
- слање порука преко симбола.

Индиректна стратегија, или стратегија когнитивне дисонанце, спроводи се тако што се путем различитих метода организације и управљања мења понашање запослених у пожељном правцу из чега следи каснија промена ставова и вредности којом се рационализују промене у понашању.

Наше је мишљење да су у области информационе безбедносне културе применљиве обе стратегије, и да их треба конбиновати у зависности од субјекта промена.

5. Унапређење културе заштите информација кроз организационо учење

Индивидуално учење је процес у којем долази до сталних промена понашања појединца, које настају као резултат искуства и стицања нових знања. Аналогно томе, организационо учење је стални процес промена које значе унапређење, иновирања и побољшања у производњи, услугама, потрошачком сервису, и другим секторима, које настају као резултат искуства и нових знања до којих је дошла једна организација, и као такво остаје увек у организацији без обзира на промене и флуктуацију запослених.[513]

Организационо учење се може дефинисати као континуирани процес стварања и усавршавања способности организација за промене.

Овај концепт доноси области заштите информација потребан квалитативни приступ, будући да због обиља претњи, које се стално иновирају, а које долазе из спољашњег и унутрашњег окружења, организације треба да стално уче о њима и свој систем заштите прилагођавају амбијенту. Процес организационог учења утиче на вредности, веровања, ставове, рутину и поступање у области заштите информација, одакле преко доминантне културе утиче на постојеће супкултуре и на тај начин унапређује свест о информационој безбедности запослених организације.

[513] *Ibid*, стр. 447. - 450.

Концепт организационог учења донео је у језик менаџмента термине: системско мишљење, креативан дијалог, тимско учење и отворио је нову перспективу за разумевање менаџерске улоге.

Неке организације уче тако што постојеће моделе понашања коригују, а друге у потпуности одбацују старе моделе и усвајају нове, али увек се полази од властитог искуства из прошлости, као и од праксе и искустава сличних организација, на основу чега се процењује сопствена способност организације за промене понашања.

Две су основне врсте учења у организацијама, адаптивно и генеративно учење.[514]

Адаптивно учење је врста учења када организација прилагођава своје понашање променама у окружењу (па смо тако сведоци учења и прилагођавања организација раду од куће запослених, изазвано *Covid* кризом, где је осим организационог прилагођавања у пуној мери изражена димензија заштите информација, о чему смо раније коментарисали у овом раду), тако што се у оквирима постојеће стратегије, дизајна и културе предузимају интервенције како би се организација прилагодила. Резултат адаптивног учења је реактивно понашање организације, што значи да се оно догађа након што су се промене у окружењу десиле, одакле су ове промене парцијалне, мале и плитке (инкременталне су природе).

Генеративно учење у суштини представља двоструко учење, и то – одучавање од старог и учење новог, одакле се односи на дубинске, велике и радикалне промене. Технолошки развој, прихватање нових технологија, промене у начину обављања пословних процеса представљају околности у којима организације приступају оваквој врсти учења, што карактерише организације високих технологија, одакле се оно односи и на банкарско пословање и пословање других финансијских институција.

Организацино учење је генеративно учење које укључује следеће технологије:[515]

- системско мишљење, где се посматра целина организације, а не само изоловани делови;
- личне вештине, које се развијају усавршавањем запослених;
- ментални модели, које чине личне представе људи о свету, појавама и процесима. То су наталожена сазнања и искуство које делују из другог плана, односно из подсвести;
- креирање визије, подразумева едукацију и оспособљавање запослених да разумеју идеју и да имају свест о њеној корисноти (као што је свест о безбедности);
- тимско учење, које представља ефекат тимског рада и чиме се унапређује начин размишљања, промена менталног модела, одбацивање предрасуда и стереотипа.

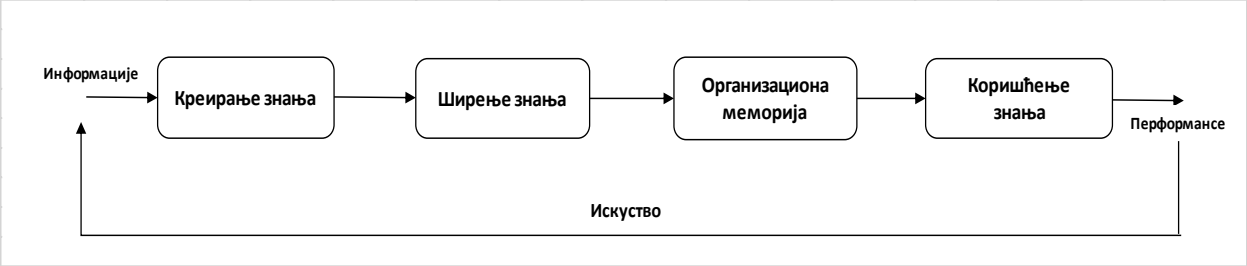
Концепт организационог учења огледа се у спремности људи да међусобно сарађују у оквиру радних тимова и група и да у интерактивним односима размењују знање и искуство и да уче и развијају своје способности.

[514] *Ibid*
[515] *Ibid*

5.1. Процес организационог учења и неке рефлексије на заштиту информација

На освноу теоријских радова из области организационог учења, неки домаћи аутори закључују да нема значајних разлика у разумевању процеса организациног учења, одакле се може формулисати интегрални модел, који садржи четири фазе: креирање знања, ширење знања кроз организацију, меморисање знања и коришћење наученог знања (Схема број 25: *Модел организационог учења*).[516]

Схема број 25: ***Модел организационог учења***[517]



Креирање знања подразумева прикупљање информација, њихову обраду и интерпретацију. Право знање је више од информација, јер садржи значење информација као и поруке које често нису очевидне.

Ширење знања кроз организацију, или дисеминација знања, подразумева да знање буде доступно свима, а што се постиже на формални начин, када се знање шири на прописан начин, применом утврђених метода, начина и средстава, и – неформални начин, када се знање преноси у неформалним односима између запослених.

Меморисање знања представља критичан фактор у процесу организациног учења. За разлику од индивидуалног учења, где је знање својина појединца, организационо знање представља ресурс организације. Организациону меморију чине писани документи, одакле произилази и значај заштите информација организације, будући да се на овај начин штити организационо знање, пре свега у односу на конкуренцију, одакле оно представља квалитативан фактор који организацију издваја на тржишту у односу на друге. У пракси, једна од опште присутних области у остваривању заштите информација јесте спречавање одлазећих запослених да у нову организацију пренесу формализова знања организације, која се састоје у интерним документима, политикама, процедурама, инструкцијама и друго, и чије преношење може да допринесе личним компетенцијама одлазећег запосленог у новој

[516] *Ibid*
[517] *Ibid*

организацији, што представља мотив за овакво безбедносно угрожавање. Такође, на овом месту се види и значај хијерархијске организованости послова заштите информација, будући да је потребно да ова пословна функција сарађује са другим, у овом случају кадровском пословном функцијом, где процес одлажења запосленог из организације треба планирати интерним документима који нису само *HR,* или безбедносне природе, већ се односе и на друге технолошке процесе, дакле на целу организацију.

Коришћење знања подразумева активности имплементације наученог. Исход ове фазе треба да буде промена понашања појединаца и промена понашања организације, или – општи пораст индивидуалних и организационих перформанси. У овој фази формира се ново искуство, које постаје извор информација у новом циклусу процеса учења, како за ту организацију, тако и за друге сличног профила (енгл: *benchmarking*[518])

Компаративна анализа, што у суштини представља *benchmarking,* представља још једну додирну тачку организације и информационе безбедности, која се огледа у потреби одржавања конкурентских предности које је организација стекла, са једне стране, и са друге стране, потребе да организацији буду доступне информације о другим организацијама.

Начин на који организације уче зависи од оријентације учења, организационе културе, претходног искуства и постојећих способности, а зависе од следећих елемената:[519]

- извора знања, који може бити интерни и екстерни. Оријентација организације на одређени извор знања указује да ли се организација бави иновацијама или имитацијама;
- фокуса учења, који може бити на производу или на процесу;
- начину меморисања знања, где треба обратити пажњу да се одласком запосленог из организације не губе стечена знања;
- начину ширења знања, где оно може да се шири формалним или неформалним путем;
- начину на који организација учи, које може бити адаптивно или генеративно;
- начину коришћења знања.

Фактори подршке учењу организације су следећи:[520]

[518] *International Group of Congroling*, одређује *benchmarking* као инструмент анализе и планирања који је заснован на упоређивању организације са конкуренцијом, и то − „најбољима у класи", али и са другим организацијама и делатностима. Применом *benchmarking*-а, постиже се унапређење квалитета производа и услуга, унапређење пословних процеса, постизање конкурентских предности и друго. Може се спроводити интерно (у оквиру организације), као и поређењем са другим организацијама. Подразумева фазе: дифинисања проблема, разумевања актуелног резултата, планирање и прикупљање података, анализу података, учење и доношење одлука о најбољем решењу и примену решења. Доступно на: https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/2004-benchmarking

[519] Петковић, М., Јанићијевић, Н., Богићевић, Б., *op.cit*., стр., 453. – 457.

[520] *Ibid*

- дизајн организације која подржава учење треба бити са малим бројем хијерархијских нивоа, са порозним границама између пословних функција и са тимским груписањем послова;
- култура организације је најважнији фактор учења и истовремено најважнији катализатор промена;
- способност афирмације, подразумева усмеравање људи да правилно процењују прошло искуство, могућности и потенцијале за будуће успехе;
- способност експанзије, људи се подстичу да изађу ван оквира познатог и да том приликом сагледају појаву коју су доживели као проблем на нов начин;
- способност за тимски рад, системско мишљење и осећај заједничке судбине – превазилази конвенционалне препреке, као што је функционална подела посла;
- способност сарадње, представља веровање да се кроз дијалог рађају нове идеје
- способност скенирања окружења, подразумева да се организација не затвара у сопствене границе;
- способност сагледавања разлика између оствареног и могућег − (енгл: *gep*) анализа;
- систем мерења и контроле, у вези са претходно наведеним;
- клима отворености, која се огледа у могућности да запослени могу да износе своје ставове руководиоцима;
- дистрибуирано лидерство, које подразумева да иницијативе треба да циркулишу у свим правцима организације.

Сви наведени фактори подршке учењу организације односе се и на учење у области заштите информација, у смислу развоја свести о безбедности, али и на ниво постигнутих резултата у остваривању заштите, будући да организација учењем утиче на организациону културу, као и да сам процес учења зависи од ње.

6. Унапређење културе заштите информација кроз спровођење организационих промена

Неки домаћи аутори наводе да се све теорије, концепти и програми организационих промена могу представити једним општим моделом, одговарајући на питања зашто долази до промена, шта се том приликом мења и како се те промене догађају (Схема број 26: *Модел организационих промена*). Одатле такав модел захтева да се сазнају узроци, садржај и процес организационих промена, које ћемо због потребе учење организације и развоја безбедносне културе, укратко приказати, будући да се на крају ових процеса увек очекују организациное промене у најширем смислу.

Организациона промена представља разлику у стању организације која настане између две временске тачке.[521]

Схема број 26: ***Модел организационих промена***[522]

6.1. Развој свети о безбедности у светлу узрока организационих промена

Развој свести о безбедности и иначе развој организационе културе, како смо претходно приказали, подразумева континуирани процес учења организације, који доводи до одговарајућих организациних промена.

Промене, односно учење нису саме по себи повод за обављање ових активности, већ су оне изазване одређеним узроцима.

Да би смо разумели узроке организационих промена морамо поћи од неких основних претпоставки, као што су:[523]

- организација је отворени систем који у циљу свог опстанка мора да обавља размену материје, енергије и информација са својим окружењем;
- организација је сложен систем чији су подсистеми у равнотежи и интерном балансу (материјални, људски, технички, структурални, информациони и други подсистеми);
- равнотежа организације је услов за остваривање њених циљева и детерминанта њених перформанси (што не важи за организације са монополским позицијама).

[521] *Ibid*, стр. 532. - 550.
[522] Ibid, стр. 536.
[523] *Ibid*

Узрок организационих промена је дебаланс равнотеже између:

- организације и окружења;
- унутар саме организације (између њених подсистема).

Организационе промене се појављују онда када дође до екстерног или интерног дебаланса равнотеже.

Есктерни узроци организационих промена обично утичу на организације индиректно, и подразумевају следеће:

- развој информационе технологије;
- глобализација светске привреде;
- промена улоге државе у привреди (неолиберална екононска политика је допринела да се значајно смањи улога државе, одакле су извршене реприватизација, денационализација и дерегулација);
- демографске промене (становништво постаје све образованије, повећана је улога жена, смањује се наталитет, становништво постаје све старије, запослени све више цене своје слободно време, а потрошачи захтевају све већи квалитет производа и услуга);
- пораст интензитета конкуренције.

Поред наведеног у теорији, на организације на овим просторима је утицало и распад заједничке државе, промена политичког система (из једнопартијског у вишепартијски), промена власништва организација и друго.

Интерни узроци организациних промена представљају оне промене карактеристика организације које захтевају прилагођавање организације, којом приликом се најчешће мисли на следеће:

- промена старости и величине организације (пролазак организације кроз животни циклус и повећање стандардизације и формализације);
- промена лидера организације (нови лидер доноси са собом нове претпоставке и веровања и намеће их осталима у организацији);
- промена власничке структуре, припајање и преузимање предузећа;
- промене развојне и пословне стратегије;
- отклањање интерних неравнотежа у структури.

Нашу пажњу посебно привлаче интерни узроци организационих промена, будући да се оне јављају у континуитету и захтевају стално прилагођавање система заштите информација у организацијама, између осталог.

У сектору банкарства, приметно је укрупњавање тржишта, одакле се јавља потреба организационих промена и проблем хармонизације различитих система у један, што подразумева и хармонизацију информационих система, али и уједначавање вредности и

ставова запослених према безбедности, истовремено са изазовима које стварају нове претње, развојм нових технологија и нових услуга које банке пружају корисницима.

6.2. Садржај унапређења културе заштите информација у контексту организационих промена

Организациони развој највећу пажњу посвећује *људском фактору*, слично као што је приступ у остваривању безбедности организације, услед чега се људи и међуљудски односи налазе модела који представља објект промена.

Поред наведеног, неки аутори су крајем осамдесетих година као објект организационих промена посматрали: стратегију, технологију и структуру, систем људских ресурса и социјалне промене у организацији.[524]

Временом, све се више елемената укључивало у овакав модел, у ком смислу је деведесетих година уведена *организациона култура*, као основни чинилац свих радикалних организационих промена.

Домаћи аутори наводе интегрални модел организације који представља основу за анализу садржаја организационих промена, према којем су пословни процеси ти који креирају перформансе. Том приликом пословни процеси се одвијају кроз оквир који представља организација, одакле она утиче на ефикасност предузећа. *Компоненте организације које чине оквир одвијања процеса* могу се поделити на две велике групе:

- структуралне (или тврде) компоненте
- бихејвиористичке (неформалне или меке) компоненте, где припадају сви облици људског понашања, као што су: култура, моћ, групе, комуницирање, стил водства и друго, одакле ова група посебно привлачи нашу пажњу због своје усредсређености на човека.

Четири су основне димензије или параметри који одређују карактер организационе структуре: подела рада, делегирање ауторитета, груписање јединица и координација. У зависности од начина на који су успостављени ови параметри формира се и профил који имплицира одређено понашање. У зависности од тога колико је наведених параметара обухваћено променама, можемо говорити о свеобухватним или парцијалним променама.

Са спекта заштите информација, наше је мишљење да су од већег значаја промене степена делегирања ауторитета и промене у груписању јединица, будући да се оне предузимају у кризним ситуацијама (као што је на пример напад на информатичке ресурсе), када лидер организације преузима ауторитет и одговорност за све одлуке и – онда када су постојеће организационе јединице постављене тако да вештачки деле природне токове

[524] *Ibid*

функционисања организације (као што је на пример неадекватна организациона позиција функције заштите информација у организацији, где је она ограничена на ауторитет пословне функције којој припада). Такође, механизам координације може бити од великог значаја за функционисање заштите информација, јер се развојем и порастом величине организације мењају и координациони механизми – од међусобног комуницирања преко хијерархијске конроле до стандардизације.

Међу системима у организацији који се најчешће мењају су информациони систем, систем планирања и контроле пословања и систем управљања људским ресурсима.[525]

Информациони систем мора да буде усклађен са организационом структуром, будући да структура одређује на којим местима се налазе извори и корисници информација. Промена структуре захтев промену информациног система јер се мења распоред и повезаност извора и корисника информације.

Наше је мишљење да се на овај начин још једном подвлачи важност заштите информација у организацији, будући да сваки поремећај у раду информационог система има за директну последицу поремећај (некада и немогућност) функционисања основних пословних процеса, јер се у том случају отежава или прекида веза између извора и корисника информација.

Систем управљања људским ресурсима обухвата планирање потреба за људским ресурсима и бројне друге активности, међу којима су и оне које су од великог утицаја на наш предмет истраживања, као што су:

- пријем нових запослених;
- тренинг и обука запослених;
- мотивација и награђивање;
- интерни трансфер кадрова.

Управљање људским ресурсима утиче директно на састав и понашање запослених, а променама система управљања људских ресурса може се ефикасно утицати на промене понашања запослених.[526]

На више места у нашем раду ми смо нагласили ову повезаност, посебно у контексту значаја свести о безбедности запослених и начинима на који се може утицати на њу.

Такође, истакли смо и значај који има *организациона култура,* која представља систем претпоставки, веровања, вредности и норми које чланови организације развијају током заједничког рада и што одређује начин њиховог мишљења и понашања. На самом почетку овог поглавља ми смо истакли значај информационе безбедносе културе, а током каснијих разматрања показали смо да је реч о супкултури доминантне културе организације.

До промена организационе културе долази услед истих разлога због којих се меса и читава организација (што је можда још један аргумент у истицању значаја организационе културе)

[525] *Ibid*
[526] *Ibid*

– промене у окружењу, раст и развој предузећа, технолошке промене и промене лидера. Ове промене могу бити различите по својој обухватности и по својој дубини захватања. У ширем смислу, представљају промене у схватању већине питања функционисања организације.

Ужи смисао промена организационе културе подразумева промене у уском сегменту претпоставки, веровања, вредности или норми понашања, одакле се овај смисао директно односи на развој свести о безбедности запослених (енгл: security awareness).

Плитке промене организационе културе подразумевају само промене неких културних норми и симбола, док се стварне вредности, веровања или претпоставке људи не мењају.

Дубоке промене културе захтевају промене најдубљих, подсвесних веровања и претпоставки о свету који нас окружује. [527]

У свакој организацији се формира и одређена структура моћи, која интегрише формални ауторитет са неформалним изворима моћи. Свака организациона промена компоненти организације изазива и померања у структури моћи (неки појединци и групе губе, а неки добијају на моћи).

Наша је мишљење да је од посебне важности за заштиту информација разумевање феномена *неформалних група*, као облика организације где запослени задовољавају неке потребе које се не могу задовољити у формалним групама. Некада став неформалне групе може бити тако изражен у организацији, да промене структуре и система могу остати без резултата у променама понашања запослених, уколико је став неформалне групе доминантан. Последично, то значи да се утицајем на ставове неформалних група може доћи и до жељених промена у понашању запослених, без промена структуре и система организације.

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

Већина модела организационих промена који се проналазе у литератури заснивају се на моделу који је развио Левин (енгл: *Kurt Lewin*), и који се одвија у три фазе:[528]

- фаза одмрзавања;
- фаза покрета или промена;
- поновно замрзавање.

Ове активности се групишу у десет корака, и то:

- стварање и ширење свести о неопходноси промена;

[527] *Ibid*
[528] *Ibid*, стр. 565. - 566.

- креирање визије нове организације;
- изградња водеће коалиције за промене;
- стварање услова за промене;
- спровођење првог циклуса промена и креирање почетних успеха;
- консолидација учињених промена и спровођење даљих промена;
- подршка промени понашања запослених;
- мониторинг и освежавање промена;
- стабилизација нове организације и њено укључивање у културу;
- осигурање успешне сукцесије.

За потребе нашег рада приредили смо табеларни преглед фаза и корака модела процеса организационих промена (Табела број 13: *Преглед фаза и корака модела процеса организационих промена*)**.**

.

Табела број 13: ***Преглед фаза и корака модела процеса организационих промена***

Фаза организационе промене	**Кораци у остваривању промене**
Одмрзавање	Стварање и ширење свести о неопходности промена
	Креирање визије организације
	Изградња водеће коалиције за промене
	Стварање услова за промене
Промена (покрет)	Спровођење првог циклуса промена и креирање почетних успеха
	Консолидација учињених промена и спровођење даљих промена
	Подршка промени понашања запослених
Замрзавање	Мониторинг и освежавање промена
	Стабилизација нове организације и њено укључивање у културу
	Осигурање успешне сукцесије

Наше је мишљење да је од посебне важности за спровођење успешних промена организације, у сфери развоја свести о безбедности, откривање извора отпора променама, која се јавља у кораку подршке промени понашања запослених.

Ради ефикаснијег савладавања отпора променама треба имати на уму следеће принципе:[529]

- отпори су природни и неизбежни, одакле их треба очекивати;
- отпори се не показују увек експлицитно и отворено, одакле их треба пронаћи;
- има много врста отпора, а показују га и они који гуве и они који добијају променама;
- људи најчешће на промене реагују емоционално, а не треба реаговати логиком на емоције;
- има више начина да се савладају отпори.

Извори отпора променама могу бити индивидуални и организациони, а према следећем:

- Индивудуални извори променама потичу од појединца, члана организације, и подразумевају следеће појаве:
    - навика, рутина, инерција (људи су по природи инертни);
    - сигурност (свака промена уноси несигурност);
    - страх од непознатог (људи се природно плаше непонатог);
    - страх од некомпетентности;
    - страх од губитка посла, позиције или моћи;
    - недовољно информација (када изостају потребне информације отпор пружају и запослени који променама добијају);
    - повећање обима посла (запослени одбијају промене јер им оне доносе више посла, или обавеза)
    - убеђење да промене нису добре за организацију (легитиман извор отпора)
- Организациони извори отпора променама:
    - структурала инерција (организацији је било потребно доста времена да научи како да обавља своје процесе, слично као што појединац има отпор да мења дневне рутине. Поред тога, процеси у организацији су повезани, и промене у једним процесима природно имају ефекат на друге, што ствара отпор);
    - структура моћи (обично промене изазивају померања у структури моћи, јер док једни добијају променама, други су на губитку. Зато они који имају моћ настоје да блокирају сваку промену);
    - организацина култура (промене се интерпретирају у складу са важећим системом вредности организације, одакле се јавља јаз између пожељног и постојећег стања и онемогућавање промене);
    - неформалне групе (што је степен кохезивности групе већи, већи је и отпор променама).

[529] *Ibid*, стр. 583. - 585.

Стратегије за савладавање отпора, природно, зависе од самих извора отпора променама, одакле је могуће применити следеће начине превазилажења ових отпора:

- стратегија информисања, комуницирања и индоктринације;
- стратегија образовања, учења, тренинга (подразумева стицање компетенција запослених и захтева велике ресурсе, али је и врло ефикасна);
- стратегија кооптације (укључивање у процес промена оних актера за које се процени да су моћни и који због тога могу да угрозе процес промена);
- стратегија преговарања и компромиса (подразумева давање уступака онима који имају моћ, да би се добила сагласност за промене);
- стратегија манипулације (врло је ризична и подразумева прикривање неких информација које треба да убеде запослене да прихвате промене. Ризик се састоји у откривању запослених, после неког времена, да су били изманипулисани. Из тих разлога у променама могу да се ангажују независни експерти, у чије се мишљење по природи ствари не сумња, због њихових компетенција);
- стратегија принуде (претње санкцијама уколико се не прихвате промене).

Област организационих промена је од суштинске важности за функционисање заштите информација у организацији, будући да смо претходно у раду видели да се ризици и претње које се јављају не само бројне и разноврсне, већ се и јављају у стално новим формама и облицима.

Из ових разлога, заштита информација је процес који се стално мења и подразумева учешће свих припадника и организационих јединица организације, у складу са њиховим учешћем у процесу остваривања заштите информација, и – у складу са могућим ризицима које они могу представљати у случају њиховог непридржавања безбедносних правила. Такође, заштита информација је и континуирани процес који подразумева промене у претпоставкама, веровањима, вредностима и нормама које чланови организације развијају у међусобним односима, што видели смо, суштински представља организациону културу, одакле опет није могуће равијати ова два концепта, заштиту информација и културу организације, одвојено, већ су оне у великој мери међусобно повезане.

7. Закључна разматрања поглавља

Информациона безбедносна култура је неодвојиви садржај у анализи заштите информација у банкама и другим финансијским институција, будући да смо прегледом референтних научних радова установили да се заштита информација бави људима, процесима и технологијом, а да се у феноменолошком приступа изучавања ове појаве сусрећемо са појмом организационе културе која утиче на брзину промена.

Такође, видели смо да је подизање свести о информационој безбедности (енгл: *security awareness*), могуће организовати преко организационе културе, као и да је стандардом ISO 17799 (односно касније ISO/IEC 27002) едукација корисника за заштитиу информација један од кључних фактора у остваривању заштите информација.

Никерк износи да заштита информација зависи од људи, и да неговање организационе супкултуре безбедности информација је неопходно у организацији, полазећи од концепта промене корпоративне културе.[530]

Према мишљењу Стајића и сарадника, безбедносна култура представља скуп усвојених ставова, знања, вештина и правила из области безбедности, испољених као понашање и процес, о потреби, начинима и средствима заштите личних, друштвених и међународних вредности од свих извора, облика и носилаца угрожавања, без обзира на место или њихово време испољавања. Безбедносна култура је у тесној вези са нашим васпитањем, вредносима и вредносним системима које подржавамо.[531]

Проблем одређивања концепта информационе безбедносне културе је данас врло присутан у научним радовима, а ми смо приказали у нашем раду да се најновији концепти заштите информације у банкама и финансијским институцијама, кроз увођење појма резилијентности, базирају на развоју свести запослених и на развоју безбедносне културе.

С тим у вези, приказали смо овогодишњи научни рад интернационалне групе аутора, где се одређује садржај информационе безбедносне културе и где је као резултат истраживања понуђен одговарајући модел, који смо приказали у оквиру овог поглавља, а из којег следи да култура информационе безбедности зависи од бројних спољашњих и унутрашњих фактора, међу којима истакнути значај имају национална култура, ниво развијености организационе културе, лидерство, прихватање промена у организацији, култура ризика у организацији, понашање запослених, њихов тренинг и личне вредности које укључују и знања о информационој безбедности.[532]

---

[530] Niekerk, J.F.: *Establishing and information security culture in organizations: an outcomes based education approach*, Dissertation submitted in fulfillment of the requirements for the degree Magister Technologiae in Information Technology, Faculty of Engineering, Nelson Mandela Metropolitan University, University in Port Elizabeth, South Africa, 2005.

[531] Миловановић, З., Радовановић, Р.: *Информацино-безбедносна култура – императив савременог друштва*, журнал за криминалистику и право БНП, Криминалистичкко-полицијска академија, Београд, 2015. година, стр. 47. – 48.

[532] Veigaa, A., Astakhova, Lj. V., Bothac, A., Herelmanc, M.: *Defining organisational information security culture—Perspectives from academia and industry*, Computer & Security, Volume 92, May 2020. Доступно на: https://www.sciencedirect.com/science/article/pii/S0167404820300018?via%3Dihub

Приказали смо и истраживање односу између кулутуре и информационе свести, где су изнети научни докази да постоји значајан позитиван однос између организационе културе, културе безбедности и информационе безбедности. [533]

На основу свега наведеног, приредили смо осврт на основне теоријске поставке организације као научне области, где смо прегледом литературе закључили да је теорија углавном сагласна да су се данас издвојиле три кључне области, и то: организациона теорија и дизајн, организационо понашање људи и организационе промене и развој и са чим у вези смо дали табеларни преглед ових области и њихов однос према области заштите информација.

Даљи приказ ових области дали смо у контексту нашег предмета истраживања, па смо тако обрадили основне теоријске поставке организационог понашања, којом приликом смо приказали модел организационог понашања, организационе културе, безбедносне културе, промене безбедносне културе, организационог учења и организационих промена.

Нагласили смо изворе отпора променама, као личне и организационе, полазећи од предпоставке да отпори промена у организацији највише могу да опструишу напоре организације да утичу на претпоставке, веровања, вредности и норме понашања запослених, што у крајњем има негативан утицај на културу организације, те на ниво информационе безбедносне културе.

[533] Wileya, A., McCormac, A., Čalić, D.: *More than individual: Examing the relationchip berween culture and information security Awareness,* Computer & Security, Volume 88, january 2020, доступно на: https://www.sciencedirect.com/science/article/pii/S0167404819301841

V ЗАКЉУЧНА РАЗМАТРАЊА

Савремену економију карактерише глобална повезаност националних и регионалних економских система, где пословање банака и других финансијских институција има кључну улогу у остваривању овог система. Пословање банака у великој мери зависи од очувања њених ресурса, где информације чине један од кључних чинилаца. Нова технолошка револуција, која се огледа у дигитализацији свих сегмената друштва, потенцира улогу и значај које имају информације за пословање банака и других финансијских институција, што се огледа у две основне и међусобно супротсављене чињенице. Прво, пословни процеси у банкама и финансијским институцијама неби могли да се обављају без обраде података и информација, што није новост, али процес дигитализације потенцира значај ових ресурса, посебно јер технолошки напредак чини да се информације гомилају а да њихово коришћење подразумева све бржу обраду и већу доступност корисницима. Друго, информације не представљају само ресурс без којег пословање неби било могуће и ресурс који доноси вредност, већ оне представљају и поље из којег долазе претње које угрожавају пословање, не толико због своје природе, колико због информатичких ресурса организације чије је сврха обрада тих информација и без којих у савремено доба информације неби имале употребну вредност на садашњем нивоу.

Предмет истраживања рада је заштита информација у банкама и финансијским институцијама, посматрано са аспекта организационог и нормативног уређења ове области.

Два су основна разлога која су нас навела на овакав избор: несумњив је значај нормативне и организационе уређености система као претпоставки успешног функционисања пословних функција, дакле и функције безбедности система, и – опазили смо у практичном остваривању ове области тренд поистовећивања области заштите информација (енгл. *Information Security*) са информатичком заштитом (енгл. *IT security*), што у имплицира запостављање других сегмената система безбедности, и одакле се последично систем безбедности јавља као некомплетан и на тај начин више рањив.

Теоријски радови у области заштите информација који се јављају двадесетак година уназад, примећују наведену недоследност и често потенцирају да се у безбедносним политикама заштите информација запоставља друштвени карактер овог феномена.

Информациони систем обрађује информације на три нивоа: техничком, формалном и неформалном. Оно што припада области информационих технологија (софтвер, хардвер, подаци и мрежне компоненте) припада техничком нивоу; документа, безбедносне стратегије, политике, упутства, смернице, стандарди и друго) припадају формалном нивоу, док – понашање људи (култура, норме, веровања, ставови, неформална комуникације и

друго) припада неформалном нивоу (Схема број 1: *Нивои информационог система према Дилану*).[534]

Овакав приступ проблему истраживања заштите информација близак је нашем приступу проблему истраживања, где је организационо и нормативно уређење заштита информација садржај формалног и неформалног нивоа информационог система.

Хипотетички оквир истраживања формулисали смо кроз претпоставке да се заштита информација у банкама и финансијским институцијама базира на информационој (*IT)* безбедности, чиме се имплицира развој других неопходних аспеката овог система заштите, а посебно у организационом и нормативном смислу. Стручњаци који се баве пословима заштите информација имају превасходно техничко формално образовање и немају едукацију из области опште безбедности. Организациона структура и систематизација организације утичу на профилисање система заштите и одређују његову ефикасност. Услови уске специјализације система заштите на технички ниво знања чине да се запостављају друге области које подразумева ефикасан безбедносни систем. Нормативно организовање послова заштите информација у банкама и финансијским институцијама базира се на стварању јединствених основа кроз израду и прихватање формалних докумената, који треба да стандардизују поступке запослених у заштити информација и да омогуће остваривање контролне функције.

Прегледом релеватних научних радова, којом приликом нисмо пронашли домаће радове који се експлицитно односе на предмет нешег истраживања, услед чега смо анализирали претежно иностране научне радове, у највећем броју докторске тезе настале у последњих петнестак година, добили смо добре претпоставке за даљи ток истраживања, а као најзначајније закључке за наш предмет истраживања издвајамо:

- заштита информација подразумева активности које се односе на људе, процесе и технологију;
- људи су најслабија карика у ланцу остваривања заштите информација;
- безбедносна култура организације у значајној мери доприноси заштити информација;
- кључну улогу у култури информационе безбедности има пословодство организације, које заједно са запосленима утиче на вредности организације које су некада видљиве а некада не;
- организационе промене имају значајну улогу за остваривање заштите информација;
- нормативни оквир заштите информација утиче на свест о бебедности корисника (енгл: *security awareness*);

[534] Harris. M. A.: *The shaping of manager's security objectives through information security awareness training*, PhD dissertation, Virginia Commonwealth University, 2010, стр. 9. позива се на извор: Dhillon, Gurpreet: *Principles of Information Systems Security: Text and Cases*, John Wiley & Sons, 2007.

- нормативни и организацнони аспекти у остваривању заштите информација се међусобно прожимају, јер се примена норми огледа у свести о безбедности, која је фундаментална за организацију и њену културу;
- недостатак безбедносне културе је уочљив и на индивидуалном и на нивоу организације;
- појавни облици и број напада на информационе системе је у порасту и тај тренд ће се наставити;
- у структури информационих инцидената учешће запослених тих организација јавља се у значајној мери;
- у остваривању заштите информација важно је учешће више пословних функција организације, а не само безбедносна пословна функција – потребан је мултидисциплинарни приступ;
- подизање свести о информационој безбедности је могуће остварити преко организационе културе, као механизма контроле. Када у организацији постоји безбедносна култура, аспекти информационе безбедности се реализују као природан, рутински и свакодневни приступ од стране запослених;
- информациона безбедност се не може затварати у технички аспект и специфична IT знања, већ је потребно да она има активну сарадњу са другим пословним функцијама, а пре свега са другим сегментима система безбдности;
- безбедност информација је вишедимензионална дисциплина, а већина тих димензија је нетехничке природе;
- едукација корисника за заштиту информација један је од кључних фактора у остваривању заштите информација и у том смислу обично се говори о развоју безбедносне свести (енгл: *security awareness*);
- безбедност информација зависи од људи, а тренутни програми о развоју безбедносне свести не придају довољно пажње теоријама понашања;
- неговање супкултуре безбедности информација не неопходно у организацији. У теорији је добро проучен проблем промене корпоративне културе, али је недовољно проучен процес промене супкултуре заштите информација;
- тренинзи (обуке) информационе безбедности су углавном техничке природе, јер су безбедносне политике исте такве. Разлог за то је што се менаџери заштите информација претежно ослањају на јавно доступне смернице, политке и стандарде, које су такође техничке природе, па услед недостатка о општим знањима из безбедности писању докумената приступају рутински, користећи туђа решења и неразумевајући шири контекст безбедности.

Полазећи од наведеног, можемо да закључимо да је досадашња теорија уочила да се у приступу и реализацији заштите информација недовољно посматрају нетехнички аспекти, који су можда и кључни за успешно остваривање овог концепта, будући да систем заштите информација у организацији зависи од великој мери од организационог и нормативног уређења ове области, од организационе културе, развоја безбедносне културе и успостављања одговарајућих тренинг програма који требају бити засновани на

познавању ширег аспекта безбедности и засновани на педагошким принципима образовања одраслих.

У поглављу о информационој безбедности дали смо преглед основних појмова који су од значаја за разумевање ове области и на истом месту смо дали преглед и анализу појединих решења организовања послова заштите информација у организацијама.

Констатовали смо да је данас у употреби велики број термина који се суштински односе на заштиту информација, те да неких од њих представљају синониме, а неки не. Анализом смо показали да је данас у порасту употреба термина сајбер безбедност (енгл: *cyber security*), са синонимом IT безбедност (енгл: *IT security*) на рачун термина информационе безбедности (енгл: *information security*) – и поред чињенице да се приликом осврта на значење ових термина под термином сајбер безбедности (кибер безбедности) подразумевају (само) ресурси којима се приступа путем сајбер простора, док заштита информација, као шири појам, обухвата све информације, независно да ли су оне у дигиталној или аналогној форми.

У раду смо дали наше објашњење ове појаве, према следећем могућем оквиру за дискусију:

- у сајбер простору је доминантан енглески језик (лингва франка[535]), и то према неким подацима чак пет пута више од других језика;
- објављени стандарди, примери најбоље праксе и друга документа из области заштите информација изворно су на енглеском језику. У говорном језику, због упућености домаћих стручњака за заштиту информација на самоучење, обично се преузимају кључни термини у изворном облику, дакле на енглеском језику, одакле се ствара „нови језик" струке, а што можемо да приметимо и код неких других професија, као што су *IT* област или банкарство[536];
- у области заштите информација доминирају стандарди који долазе из техничког подручја;
- искуствено опажање нас упућује на закључак да је кадровска структура стручњака за заштиту информација таква да је њихово формално образовање углавном

[535] У онлајн верзији речника *Oxford Advanced Learner's Dictionary,* (лат: *lingua franca*) је дефинисан као језик који је усвојен као заједнички језик међу говорницима чији је матерњи језик различит. Користе га неизворни говорници, који имају различите лингвистичке и културне позадине. Не ради се о језику за посебне намене, нити о пиџину или међујезику. Дакле, лингва франка је језик за комуникацију. Пиџин је језик сторен на бази речника и структуре једног језика. Користи се када нема заједничког језика између група.

[536] Да ово није усамљен пример говори нам лингвистичко истраживање, управо у области банкарства у Републици Србији. Пронађено је више од 800 термина који се користе у банкарству (а да имају контакт са енглеским језиком) и сваки од њих је анализиран у оквиру педесет различитих лингвистичких категорија. Резултати показују да је реч углавном о преузимању термина из енглеског језика, а не о превођењу. Аутор наводи да је енглески језик лингва франка (лат: *lingua franca*) светске банкарско-финансијске заједнице, а да са друге стране наш језик има значење у комуникацији локалног типа, те да је под снажним утицајем енглеског језика, али и да га краси небрига од стране корисника. Резултат истраживања је речник у којем је садржано око 400 стандардизованих термина српског језика банкарства и финансија – дакле предлог термина које нема потребе изговарати на страном језику, што је половина термина обухваћених истраживањем. Више о томе: Александар Ђ. Вулетић, *Контакти енглеског и српског језика у области банкарства и финансија*, докторска дисертација, Филолошки факултет, Универитет у Београду, Београд, 2013. године, доступно на: http://nardus.mpn.gov.rs/bitstream/handle/123456789/4044/Disertacija.pdf?sequence=1&isAllowed=y

техничке природе (јер се заштита информација, оправдано или не, везује за сајбер простор), што је тврдња коју тек треба доказати;
- нормативни оквир заштите информација, када је у питању домаћа пракса, долази од стране институција и органа Европске уније, дакле на енглеском су језику, одакле се приликом превођења на српски језик користе термини створени у „новом језику" струке;
- америчке софтверске компаније су најбројније у свету, одакле се не може игнорисати њихов интерес ширења тржишта (што важи и за област заштите информација), а меркетиншки је прихватљивије целу област називати сајбер простором, јер и сами производи и услуге које нуди ова индустрија долазе из сајбер простора;
- у САД термин сајбер безбедност (или *IT* безбедност) је двоструку чешће у употреби од термина информациона безбедност, одакле се он последично, преко производа, трансфера знања, стандарда струке и друге документације која чини нормативни оквир заштите информација преноси даље, као неформални стандард струке.

Имајући у виду наведене аргументе, ми смо се определили да у раду користимо оне термине на које нас наводе наши извори истраживања, којом приликом смо се трудили да задржимо свест о суштинској разлици у поимању ових термина на местима где је то опредељујуће за процес закључивања.

У овом поглављу дали смо историјски преглед развоја области заштите информација, почевши од шездесетих година прошлог века (појава масовније употребе рачунара), јер смо сматрали да је важно како за наше истраживање, тако и за будућа, да се разуме континуитет праћења посматраног феномена.

Последња декада, бележимо стални развој технологије, али и напада. Инциденти изазвани злонамерним активностима су постали све чешћи, све обимнији и са више нанете штете. Најпознати су: Афера Сноудена са Националном безбедносном агенцијом, НСА (енгл: *Edward Snowden & National Security Agency − NSA*), 2013. године, бивши запослени ЦИА-е (енгл: *CIA*), копирао је и објавио податке НСА, исгичући чињеницу да је влада шрijунирала јавност; Yahoo, 2013. – 2014. године, хакери провалом угрозили рачуне и личне податке великог броја корисника, због чега је компанија кажњена са 35 милиона долара (нису благовемено објавили компромитацију података), а цена компаније је на берзи опала за 350 милиона долара; *WannaCry,* 2017. године, напад је општепознатији као први рансомворм (енгл: *ransomworm*), где су мета били рачунари са Мајкрософтовим Виндоус оперативним системом (енгл: *Microsoft Windows operating system*), где се откупнина плаћала у криптовалути Биткоин. За само један дан, заражено је преко 230 хиљада рачунара у 150 земаља, итд.[537]

[537] Доступно на: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

Домаћи аутори наводе да на основу искустава добре праксе у остваривању заштите информација треба користити *модел вишеслојне заштите*, који представља вид проактивног деловања и обухвата неколико аспеката, и то: [538]

- физички (онемогућава физички приступ - физичко обезбеђење);
- технички (техничко обезбеђење - електронско обезбеђење; заштита од електромагнетног зрачења; идентификација, верификација и ауторизација приступа; системи за детекцију и спречавање напада; криптографија);
- организациони (организациона структура, дефинисање радног процеса, развој софтверских система, праћење смерница и стандардâ, планирање итд);
- кадровски (планирање и избор кадрова, руковођење, стручно усавршавање и безбедносно образовање итд.);
- нормативни (закони, упутства, планови и друга регулатива која обавезује и прописује извршење неке радње и начин изршења те радње).

У нашем истраживању ми смо обухватили већину наведених аспеката, не придржавајући се круто наведене поделе, већ смо ове садржаје дали кроз анализу у одговарајућим поглављима, где смо сматрали да је пригодно да организациони аспект буде садржан у више припадајућих логичких целина, па смо га разматрали у оквиру овог поглавља, али и у оквиру поглавља о информационој безбедносној култури. Слично смо поступили са нормативним уређењем заштите информација, па је оно тематски садржано у овом поглављу, као и у посебној тематској целини.

На овај начин желели смо да покажемо прожимање организационих и нормативних, односно других области у остваривању заштите информација, сматрајући да такав приступ одговара комплексној и мултидисциплинарној природи заштите информација.

Као прилог овој тврдњи, у оквиру поглавља дали смо и преглед основних функција које треба да буду укључене у систем заштите информација организације и то не нужно у оквиру безбедносне функције организације, али смо наведели да је потребно имати их „негде" у организацији.

Кроз процес истраживања дали смо неколико карактеристичних модела организовања послова заштите информација у организацији, где смо напоменули да их треба посматрати начелно, а не као конкретне и у том смислу обавезујуће. Анализирани су следећи могући модели организовања послова заштите информација, и то:

- у оквиру IT послова;
- у оквиру пословне функције безбедности;
- у оквиру општих послова;
- у оквиру послова стратегије и развоја;
- у оквиру правних послова;
- у оквиру послова осигурања и управљања ризиком;

[538] Цигурски, О.: *Информационе технологије у борби против тероризма*, Зборник Факултета цивилне одбране, Београд, 2005, стр. 179.

– у оквиру других пословних фукција.

Закључили смо да послове безбедности треба организовати на такав начин да обухватају целу организациону структуру, али да не буду распршени по различитим пословним функцијама, а посебно да у области заштите информација не буду организовани тамо где је могућ и очекивајући сукоб интереса, као што је то био модел где су ови послови организовани у пословној функцији IT-а. Избор одговарајућег модел зависи од више елемената, у које могу да спадају: врста индустрије којој припада организација, национална култура (безбедносна култура), географски простор са својим економским особинама тржишта, нормативни оквир, величина организације, старост организације (да ли је пословни субјекат на почетку свог деловања или је присутан већ неко време на тржишту), степен криминалитета окружења, организациона култура, расположиви људски ресурси, пословни циљеви организације, величина буџета организације и друго.

Безбедност не треба посматрати као готов производ, већ је то процес, који треба прилагођавати условима амбијента у којем се налази, одакле и организационо уређење заштите информација треба развијати као сталан организациони процес.

У поглављу о нормативном организовању послова заштите информација у банкама и другим финансијским институцијама пошли смо од потребе да нормативни оквир треба посматрати на међународном и домаћем нивоу. Такође, на нивоу организација, претходно смо нагласили да нормативни оквир чине различити документи, са својим међусобним везама и односима, од који се издвајају безбедносне политике, стандарди, упутства, смернице, процедуре и друго, те смо у том смислу представили модел хијерархије нормативних докумената организације.

Препознали смо да постоје извесна одступања када је у питању терминологија у називу докумената који чине нормативни оквир организација код остваривања заштите информација, како смо то до сада навели, и – домаће номенклатуре интерних аката који се доносе у организацијама, али смо нагласили да у нашем раду немамо амбицију да решавамо овај проблем, већ да ћемо користити ону терминологију, како нам то наводе наши извори истраживања.

Анализирајући нормативни оквир, истраживање смо конципирали тако да смо кренули од уставних и законских оквира заштите података, интерних аката правног лица и процене ризика у заштити података, па смо преко давања прегледа основних појмова који се односе на банкарско пословање приказали домаћи и међународни нормативни оквир у остваривању заштите информација у банкама и финансијским институцијама.

По својој важности и односом са предметом истраживања, издвајају се Закон о банкама, Одлука о минималним стандардима управљања информационим системом финансијске институције и Одлука о управљању ризицима банке.

Закон о банкама експлицитно наводи да банка идентификује, мери и процењује ризике којима је изложена у свом пословању и управља тим ризицима, а Члан 29 препознаје *оперативне ризике*, укључујући правни ризик, као и ризик неодговарајућег управљања

информационим и другим технологијама значајним за пословање банке. Такође, закон одређује и појам банкарске тајне као пословне тајне, што је регулисано одељком о тајности података.

Посебну важност за нормативно уређење заштите информација у банкама и финансијским институцијама има *Одлука о минималним стандардима управљања информационим системом финансијске институције*, будући да се овим документом утврђују следеће обавезе[539]:

- израда стратегије развоја информационог система;
- израда политике безбедности информационог система;
- израда Плана континуитета пословања (енгл: *Business Continuity Plan*);
- израда Плана опоравка активности у случају катастрофа (енгл: *Disaster Recovery Plan*);
- оспособљавање резервне локације за опоравак информационих система (резервни рачунарски центар);
- обавеза да се најмање једном годишње тестирају наведени планови, а да се документовани резултати тестирања доставе надлежном органу;
- обавеза адекватног, континуираног стручног оспособљавања и обучавања запослених за коришћење информационих система и очување његове безбедности и функционалности.

Народна банка Србије прописује ближе услове и начин идентификације, мерења и процене ризика којима је банка изложена у свом пословању, осим ризика усклађености пословања, *Одлуком о управљању ризицима банке,* према следећем:[540]

- банка је дужна да успостави такву унутрашњу организацију, односно организациону структуру којом ће активности управљања ризицима (енгл: *middle office*) и активности подршке (енгл: *back office*) функционално и организационо одвојити од преузимања ризика (енгл: *frong office*), с јасно утврђеном поделом послова и дужности запослених којом се спречава сукоб интереса;
- банке су дужне да усвоје и примењују стратегију развоја информационог система и политику информационог система;
- банке су је дужна да идентификују и процене догађаје и изворе због којих могу да настану губици у вези са оперативним ризицима, узимајући у обзир све значајне унутрашње и спољне факторе;
- ради обезбеђивања континуитета пословања управни одбор банке је дужан да усвоји план континуитета пословања (енгл: *Business Continuity Plan – BCP* план), као и план опоравка активности у случају катастрофа (енгл: *Disaster Recovery Plan – DRP* план).

[539] „Службени гласник РС“, бр. 23/2013, 113/2013, 2/2017 и 88/2019

[540] „Службени гласник РС, бр. 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 – др. одлука 1, 43/2013, 92/2013, 33/2015, 61/2015, 61/2016, 103/2016 и 119/2017

На међународном плану, по свом значају издвајају се Базелски споразуми (I, II и III), а посебно Базел II споразум, будући да он третира оперативни ризик, који је од кључног значаја за област заштите информација у банкама и финансијским институцијама.

На основу Базел II Народна банка Србије је донела одговарајућа акта (објављена у „Службеном гласнику РС“, бр 45/2011 и 46/2011).[541]

Од посебне важности за наш предмет истраживања, јесте истицање *значаја подизања свести запослених и културе понашања* у односу на изложеност оперативним ризицима, од стране Базелског комитета, као једног од приоритета у управљању оперативним ризицима.

Савремени концепт остваривања заштите информација у банкама изложили смо кроз *приказ резилијентности информационих система у банкама и финансијским институцијама*, што представља допринос нашег истраживања како домаћој теорији, тако и практичарима који обављају ове послове.

Непредвидивост, екстремна несигурност и брзи развој потенцијала сајбер претње стварају ситуацију у којој је процена ризика све више неспособна да пружи адекватне одговоре који се односе на сајбер безбедност великих система, а посебно критичних инфрастуктура. Једина одговарајућа одбрана, била би одвајање сајбер система од интернета, на исти начин на који биолошки системи развијају имунитет од инфекција и других напада, одакле се и сајбер системи морају прилагодити на сличан начин.

Cyber Resilience, је предвиђање и прилагођавање променама у окружењу, задржавање и брзи опоравак од сајбер инцидента, наводи Сајбер лексикону који је издао Одбор за финансијску стабилност (енгл: *Financial Stability Board – FSB*).[542]

У раду смо представили документ о сајбер резилијентности финансијске тржишне инфраструктуре, издат од стране Банке за међународна поравнања (БИС) и Међународне комисије за хартије од вредности (ИОСЦО), на основу чега смо приредили преглед садржаја компоненти и категорија сајбер резилијентности, што може помоћи будућа истраживања на овом пољу, а такође може користити и практичарима у банкама који раде на пословима заштите информација.

Сајбер резилијентност у банкама и финансијским институцијама подразумева да:

- заштита мора да обухвата информатичке ресурсе, али и заштиту људи и процеса;
- да савремени концепт заштите обухвата и мере нетехничке природе, а посебно да у том смислу обухвата знања која долазе из менаџерских наука о управљању, планирању, организационој култури, едукацији запослених и сл.;

[541] Доступно на: https://www.nbs.rs/internet/latinica/55/55_2/55_2_3/o_propisima_bazel_II.pdf

[542] ФСБ је тело које су основали шефови фржава и влада Г 20, у циљу промоције реформе међународне финансијске регулације и надзора. Доступно на: https://www.fsb.org/2018/07/cyber-lexicon-consultative-document/

– да савремени концепт заштите информација обухвата и неке традиционалне области безбедности, као што су физичко-техничка заштита, безбедносне провере, безбедносне истраге и друго.

У оквиру приказа међународних стандарда који се односе на заштиту информација дали смо приказ фамилије стандарда из серије ISO 27000, будући да они чине оквир за управљање заштитом информација (енгл: *Information Security Management System – ISMS*). Посебно, анализирали смо стандард ISO/IEC 27002, будући да он обухвата, између осталог, и организовање заштите информација у организацијама и законску усклађеност, одале се односи на организационо и нормативно уређење заштите информација.Такође, упутили смо и на друге стандарде који се могу користити у заштити информација, као што су: *COBIT,* серију стандарда које је издао *NIST,* специфичпне стандарде као што су *PCI DSS* и Уредба Европског парламента о заштити појединаца у вези са обрадом личних података и слободном кретању таквих података (енгл: *General Data Protection Regulation – GDPR*).

Полазећи од наведеног, поглављем о нормативној уређености заштите информација у банакама и финансијским институцијама *утвдили смо да постоје међународна и домаћа норматива којом се ствара јединствена основа за стандардизовање поступака у области заштите информација, као и одговарајући правни механизми издати од сране регулатора, а да банке и финансијске институције својим интерним актима треба да конкретизују прописана начела, и да их прилагоде конкретним условима сваке организације понаособ, укључујући при томе мере техничке и нетехничке природе у циљу заштите информација која мора да обухвата информатичке ресурсе, људе и процесе.*

Анализом појма резилијентности, доказали смо да развој свести запослених и безбедносна култура организације представљају неке од кључних елемената за остваривање савременог система заштите информација у банкама и другим финансијским институцијама, што предеставаља још једна аргумент за доказивање наше хипотезе да се заштита информација не заснива информациној (*IT*) безбедности.

Из ових разлога, у поглављу о информационој безбедносној култури, закључили смо да се на подизање свести о потреби заштите информација у организацији може утицати преко организационе културе, што је садржано као механизам и у међународним стандардима серије ISO 27000. Заштита информација у великој мери зависи од људи, одакле неговање супкултуре безбедности информација је неопходно у организацији, што се доводи у вези са променом корпоративне културе.

У оквиру овог поглавља приказали смо садржај информационе безбедносне културе и одговарајући модел, из којег следи *да култура информационе безбедности зависи од бројних спољашњих и унутрашњих фактора, међу којима истакнути значај имају национална култура, ниво развијености организационе културе, лидерство, прихватање*

промена у организацији, култура ризика у организацији, понашање запослених, њихов тренинг и личне вредности које укључују и знања о информационој безбедности.[543]

Такође, представили смо научне доказе да постоји значајан позитиван однос између организационе културе, културе безбедности и информационе безбедности.[544]

Анализом теоријских извора из организације као научне области, дали смо преглед утицаја организационе теорије и дизајна, организационог понашање људи и организационих промена и развоја на област заштите информација. У том смислу приказали смо модел организационог понашања и истражили организациону културу, безбедносну културу, промене безбедносне културе, организационо учење и организационе промене, у контексту заштите информација.

Идејним пројектом докторске дисертације, који је урађен 2013. године, било је предвиђено да се у оквиру истраживања уради и анкетно истраживање које би се спровело у банкама у Реублици Србији, како би се испитала претпоставка да се заштита информација у банкама и финансијским институцијама, у пракси базира на информационој, или *IT* безбедности, чиме се имплицира развој других неопходних аспеката овог система заштите, у смислу њиховог запостављања. Такође, наша искуствено опажање је упућивало на закључак да стручњаци који се баве заштитом информација у банкама и другим финансијским институцијама имају углавном техничко образовање, а да са друге стране немају формалну едукацију из области безбедности, што нашим истраживањем није обухваћено, али искуственим опажањем очекујемо да би се ова претпоставка потврдила спровођењем одговарајућег истраживања.

Од анкетног истраживања одустало се у поступку израде рада из више разлога, и то:

- теоријском анализом дошли смо до закључка да је занемаривање нетехничких аспеката опште присутан проблем у остваривању заштите информација у свету, одакле се као општи принцип односи и на праксу у Републици Србији;
- анализом постојећих научних радова и нормативе која се развија на дневном нивоу у свету у области заштита информација, закључили смо да савремени концепт заштите информација обухвата равноправно информатичке ресурсе, људе и процесе, односно обухвата неизоставно и мере нетехничке природе;
- на банкарском тржишту је присутан тренд укрупњавања, одакле се број банака временом смањује, чиме се смањује могући узорак истраживања. У 2013. години у Републици Србији било двадесет и девет банака, а према данашњим подацима НБС на банкарском тржишту је присутно двадесет и шест банака;[545]

[543] Veigaa, A., Astakhova, Lj. V., Bothac, A., Herelmanc, M.: *Defining organisational information security culture—Perspectives from academia and industry*, Computer & Security, Volume 92, May 2020. Доступно на: https://www.sciencedirect.com/science/article/pii/S0167404820300018?via%3Dihub

[544] Wileya, A., McCormac, A., Čalić, D.: *More than individual: Examing the relationchip berween culture and information security Awareness*, Computer & Security, Volume 88, january 2020, доступно на: https://www.sciencedirect.com/science/article/pii/S0167404819301841

[545] Подаци о броју банака у Републици Србији преузети су са сајта Народне банке Србије, доступно на: https://www.nbs.rs/internet/cirilica/50/50_2.html, приступано дана 11. маја 2020. године

– банке су по природи затворени системи за обављање спољашњих истраживања – што је посебно изражено у безбедносним пословним функцијама. Струковно удруживање на домаћем тржишту није развијено, па је изостала могућност да се такво истраживање обави преко одговарајућег еснафског удружења. Удружење менаџера безбедности у банкама које је основано 2007. године у оквиру Привредне Коморе Србије више не постоји, а једино тело које окупља менаџере безбедности у банкама и другим финансијским институцијама, у оквиру Одбора за безбедност Удружења банака Србије, окупља свега једанаест банака чланица, није показало интересовање за овакво истраживање и поред наших настојања и упућивања формалне молбе за учешћем у истраживању.[546] Такође, у случају да је истраживање спроведено, поставило би се питање репрезентативности обрађеног узорка, у зависности од броја добијених одговора једанаест банака чланица, од укупно присутних двадесет и шест на тржишту.

Полазећи од добијених резултата истраживања, сматрамо да можемо да закључимо да смо потврдили наше претпоставке изнете у хипотетичком оквиру, односно да је у потврђено да заштита информација у банкама и финансијским институцијама не може да се заснива само на информационој безбедности, већ да она обухвата и друге аспекте безбедности, а посебно нетехничке аспекте који обухватају информационе ресурсе, људе и процесе. Организациона структура знатно утиче на профилисање система заштите информација и одређује његову ефикасност, будући да систем заштите информација у банкама и другим финансијским институцијама треба да обухвата целу организацију по својој ширини и дубини, а не да буде затворен у појединим пословним фукцијама, и – нормативно организовање послова заштите информација у банкама и финансијским институцијама представља основе које треба да стандардизују поступке запослених у организацији кроз стварање формалних докумената о заштити информација и кроз развој свести о безбедности, који није могуће реализовати без видљиве подршке менаџмента овом циљу, као трајном процесу.

У будућности се предвиђа раст безбедносних ризика у области информационе безбедности, у банкама и финансијским институцијама, што ће довести до истоврене потребе уже специјализације ангажованих људских ресура по проблемским областима у оквиру безбедносне функције − и, са друге стране, до потребе мултидисциплинарног приступа у креирању потребних образовних профила за ове потребе.

Наше је мишљење да Факултет безбедности, Универзитета у Београду, полазећи од тренутних образовних садржаја, као и од расположивих кадровских потенцијала, може да на основу исказаних потреба за едукацијом стручних кадрова у области заштите информација, како је то приказано резултатима истраживања овог рада, да креира одговарајући образовни садржај и да на тај начин допринесе усклађивању потреба за развојем стручњака безбедности са потребама које намеће савремено пословно окружење.

[546] Подаци о броју банака чланица Одбора за безбедност преузети су са сајта Удружења банака Србије, доступно на: https://www.ubs-asb.com/o-nama/strucni-odbori/odbor-za-bezbednost, приступано дана 11. маја 2020. године

VI ЛИТЕРАТУРА

КЊИГЕ:

1. Алексић, Ж., Миловановић, З.: *Криминалистика*, Партенон, Београд, 1994.
2. Асанж, Ц.: *Слобода и будућност интернета*, Albion Books, Beograd, 2013.
3. Бајагић, М.: *Основи безбедности*, Криминалистичко-полицијска академија, Београд, 2007.
4. Bell, D.A.: *Information Theory and its Engineering Applications*. London: Pitman & Sons. 1957.
5. Даничић, М., Стајић, Љ.: *Приватна безбједност*, Висока школа унутрашњих послова, Бања Лука, 2008.
6. Џамић, В.: *Организационо понашање и корпоративна култура*, Универзитет Сингидунум, Београд, 2016.
7. Џелетовић, М., Живковић, А., Бојовић, П.: *Банкарски менаџмент*, Чигоја штампа, Београд, 2008.
8. Џигурски, О.: *Информатика*, Факултет цивилне одбране, Београд, 2002.
9. Fischer, R.J., Halibozek, E., Green, G.: *Introduction to Security*, eighth ed. Butterworth-Heinemann, Boston, 2008.
10. Gurpreet, D.: *Principles of Information Systems Security: Text and Cases*, John Wiley & Sons, 2007.
11. Хаџић М.: *Банкарство*, Универзитет Сингидунум, Београд, 2018.
12. Krieger, W.: *Историја тајних служби – од фараона до НСА*, Лагуна, Београд, 2016. година
13. Мандић, Ј. Г.: *Системи обезбеђења и заштите*, Факултет цивилне одбране, Универзитет у Београду, Београд, 2004.
14. Мандић, Ј. Г., *Систем обезбеђења и заштите правних лица,* Факултет безбедности, Универзитет у Београду, Београд, 2015.
15. Мандић, Ј. Г., Путник, Н., Милошевић, М.: *Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти*, Факултет безбедности, Универзитет у Београду, 2017.
16. Mitnick K, Simon W.: *The art of deception: controlling the human element of security*, Wiley Publishing; 2002.
17. Петковић М., Јанићијевић Н., Богићевић Б.: *Организација* , Економски факултет, Београд 2002.
18. Петровић, С.: *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004.
19. Post, R.S., Kingsbury, A.A.: *Security Administration: An Introduction to the Protection Services*, fourth ed. Butterworth-Heinemann, Boston, 1991.
20. Путник, Н.: *Сајбер простор и безбедносни изазови*, Факултет безбедности, 2009.
21. Ранђеловић, Д.: *Високотехнолошки криминал*, Криминалистичко-полицијска академија, Београд 2013.
22. Ранђеловић, Д.: *Основи информатике*, Криминалистичко-полицијска академија, ЈП „Службени гласник“, Београд, 2013. година
23. Ritter, S., Silver, W.L, Udell, G.E.: *Принципи новца, банкарства и финансијског тржишта*, УБС, Београд, 2009.
24. Селаковић, М. Н.: *Душанов законик и правни трансплanти*, упоредно-правна студија, Катедра за правну историју, Правни факултет, Универзитет у Београду, 2007.
25. Whitman, M., Mattord, H. J.: *Management of Information security*, Course Technology Cengage Learning, second edition, Boston, USA, 2008.

ДОКТОРСКИ И МАГИСТАРСКИ РАДОВИ:

26. Alnatheer, A.M.: *Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia*, PhD Thesis, Faculty of Science and Technology, Queensland University of Technology, Brisbane, Queensland, Australia, 2012.
27. Birkeland, S.: *E-Banking security and organisational changes*, PhD dissertation, University of Liverpool, 2015.
28. Harris, A. M.: *The shaping of manager's security objectives through information security awareness training*, PhD dissertation, Virginia Commonwealth University, 2010.
29. Khalid, F., Qureshi, M.A.: *How companies manage IT security A comparative study of Pakistan and Sweden*, master thesis in informatics, Jönköping International Business School, Jönköping University, Sweden, 2013.
30. Kinnari, J.: *Development of a Structured Security Document Framework*, Master's Thesis, Laurea University of Applied Sciences, Vantaa, Finland, 2013.
31. Koskokas, I.V.: *A Socio-Organizational Approach to Information Systems Security Management in the Context of Internet Banking*, A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing at St. John's Brunel University, London, UK, 2004.
32. Lee Botha, C.: *A Gap Analysis to Compare Best Practice Recommendations and Legal Requirements when raising Information Security Awareness amongst Home Users of Online Banking*, Submitted in accordance with the requirements for the degree of Master of Science in the subject Information Systems, University of South Africa, 2011.
33. Ковачевић, В.: *Модели управљањеа ризиком у банкарскмо сектору*, докторска дисертација, Факултет за економију и превредни менаџмет, Универзитет привредна академија, Нови Сад, 2016.
34. Мандић, Г.: *Безбедност корпоративних ресурса угрожених социјалним инжењерингом,* докторски рад, Факултет безбедности, Универзитет у Београду, 2010.
35. Марковић Петровић, Д. Ј.: *Процена безбедносног ризика у индустријским системима даљинског управљања*, докторска дисертација, Саобраћајни факултет, Универзитет у Београду, 2018.
36. Машић, С.: *Мерџери и аквизиције у европском банкарству*, докторски рад, Универзитет Сингидунум, Београд, 2009.
37. Niekerk, J.F.: *Establishing and information security culture in organizations: an outcomes based education approach*, Dissertation submitted in fulfillment of the requirements for the degree Magister Technologiae in Information Technology, Faculty of Engineering, Nelson Mandela Metropolitan University, University in Port Elizabeth, South Africa, 2005.
38. Путник, Н.: *Кибер ратовање – нови облик савремених друштревних конфликата,* докторски рад, Факултет безбедности, Универзитет у Београду, Београд, Република Србија, 2012.
39. Станаревић, С.: *Концепт безбедносне културе и претпостаке његовог развоја,* докторски рад, Факултет безбедности, Универзитет у Београду, Београд, Србија, 2012.
40. Шеховић, Д.: *Стандарди за управљање информационим системима финансијских институција*, мастер рад, Универзитет Сингидунум, Београд, 2014.
41. Tintamusik,Y.: *Examining the Relationship between Organization Systems and Information Security*, Faculty of the School of Business and Technology Management, Northcentral University, Arizona, USA, 2010.
42. Вуковић, В.: *Ризици у банкарству са посебним освртом на оперативни ризик*, магистарски рад, Универзитет Сингидунум, Београд, 2009.

43. Вулетић, Ђ. А.: *Контакти енглеског и српског језика у области банкарства и финансија*, докторска дисертација, Филолошки факултет, Универитет у Београду, Београд, 2013.

ЧЛАНЦИ:

44. Alcazar, F., Fenz, S.: *Mapping ISO 27002 into Security Ontology*, Vienna University of Technology, https://upcommons.upc.edu/bitstream/handle/2099.1/17302/memoria.pdf?sequence=4&isAllowed=y, 15.05.2020.
45. Alfawaz, S.M.: *Information security management: A case study of information security culture*, Faculty of Science and Technology, Queensland University of Technology, 2011.
46. Anderson, J.: *Introduction to Information Security*, https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf, 11.05.2020.
47. Andersson, D., Gustavsson, M., Waldén, A.: *How a bank organization handles robberies – a question of crisis management*, Jonkoping International Business scool, Jonkoping University, Sweden, 2008., http://www.diva-portal.org/smash/get/diva2:3643/FULLTEXT01.pdf, 11.05.2020.
48. *Annual cyber security and cyber insurance spending worldwide from 2015. to 2020.*, Statista, 2020., https://www.statista.com/statistics/387868/it-cyber-securiy-budget/, 11.05.2020.
49. *Banking in Europe: EBF Facts & Figures 2019*, European Banking Federation, 2019., https://www.ebf.eu/wp-content/uploads/2020/01/EBF-Facts-and-Figures-2019-Banking-in-Europe.pdf, 11.05.2020.
50. Barker, I.: *Third-party access management leaves organizations exposed*, https://betanews.com/2019/11/20/third-party-access-organizations-exposed/, 11.05.2020.
51. Бисић, В.: *Комплајанс, којим путем даље*, стручни чланак, Банкарство, 2018., vol. 47, бр. 4, https://scindeks-clanci.ceon.rs/data/pdf/1451-4354/2018/1451-43541804144B.pdf, 11.05.2020.
52. Campbell, K., Gordon, L., Loeb, M. and Zhou, L.: *The economic cost of publicly announced information security breaches: empirical evidence from the stock market*, Journal of Computer Security, Vol. 11 No. 3, 2003., pp. 431-448.
53. *Changing CISO's Reporting Structure: Why The Debate Is Back?*, CIO&Leader, https://www.cioandleader.com/article/2019/07/03/changing-cisos-reporting-structure-why-debate-back, 11.05.2020.
54. Computer Crime and Security Survey, CSI/FBI, 2003., http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf, 11.05.2020.
55. *COVID-19 Insights – Emerging Risks, Financial services sector is having to adapt rapidly, KPMG, 2020.*, https://home.kpmg/xx/en/home/insights/2020/04/covid-19-insights-emerging-risks.html, 11.05.2020.
56. *Cyber Security vs. Physical Security: What Do CEOs Care About?*, Loss Prevention Magazine, 2018., https://losspreventionmedia.com/cyber-security-vs-physical-security-what-do-ceos-care-about/, 11.05.2020.
57. Ћосић, Ј, Медић, А.: *Информацијска сигурност, стандарди и стање у институцијама у БиХ*, Зборник радова V Научно-стручне конференције Менаџмент и сигурност, Хрватско друштво инжењера сигурности и Висока школа за сигурност, Чаковец 2010.
58. Detert, J., Schroeder, R., Mauriel, J.: *A framework for linking culture and improvement initiatives in organisations*. The Academy of Management Review, https://www.researchgate.net/publication/200552256_A_Framework_for_Linking_Culture_and_Improvement_Initiatives_in_Organizations, 11.05.2020.

59. Цигурски, О.: *Информационе технологије у борби против тероризма*, Зборник Факултета цивилне одбране, Београд, 2005.
60. Ејдус, Ф.: *Опасне везе: теорија секуритизације и шмитовско наслеђе*, Безбедност западног Балкана, часопис београдске школе за студије безбедности, број 13., Београд, 2009. https://www.academia.edu/2543917/Opasne_veze_teorija_sekuritizacije_i_%C5%A0mitovsko_nasle%C4%91e, 11.05.2020.
61. *Енигма*, https://raf.edu.rs/citaliste/istorija/4336-enigma
62. *EU cyber cooperation: the digital frontline*, European Network and Information Security Agency (ENISA), 2012, https://www.enisa.europa.eu/publications/eu-cyber-cooperation-the-digital-frontline/, 11.05.2020.
63. *Financial Sector's Cybersecurity*: *A Regulatory Digest*, World Bank Group, 2019., http://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf, 11.05.2020.
64. Грегановић, Б.: *Дигитална трансформација банака није само креирање апликације – то је промена начина размишљања*, председник Извршног одбора НЛБ банке, Београд, 2019. година, доступно на: https://www.netokracija.rs/digitalna-transformacija-banke-161180, 11.05.2020.
65. Hui, K.L.: *Cybersecurity: Challenges and Recent Developments*, Department of Information Systems, Business Statistics and Operations Management (ISOM), Hong Kong University of Science and Technology (HKUST), Hong Kong, 9th International Conference on Internet Technologies & Society, 2019.; доступно на: http://its-conf.org/oldconferences/2019/wp-content/uploads/2019/02/ITS-2019-Keynote-Speech-on-Cybersecurity.pdf, 11.05.2020.
66. Јовановић, М.: *Правна норма*, предавање, Правни факултет, Универзитет у Београду, http://ius.bg.ac.rs/prof/Materijali/jovmio/Dokumenti/Pravna%20norma.htm, 11.05.2020.
67. *Информатор о раду Вишег јавног тужилаштва у Београду*, ажуриран дана 04.03.2019. године, https://bg.vi.jt.rs/informator/, 11.05.2020.
68. *Кинески просјаци новац прикупљају уз помоћ смартфона*, Независне новине, доступно на: https://www.021.rs/story/Info/Nauka-i-tehnologija/177828/Kineski-prosjaci-novac-prikupljaju-uz-pomoc-smartfona.html, 11.05.2020.
69. *Корона вирус и онлајн безбедност: како су корисничко име и лозинка за информациони систем Covid – 19 завршили на интернету*, дневне новине Данас, онлајн издање, 20.04.2020., https://www.danas.rs/bbc-news-serbian/korona-virus-i-onlajn-bezbednost-kako-su-korisnicko-ime-i-lozinka-za-informacioni-sistem-covid-19-zavrsili-na-internetu/, 11.05.2020.
70. Kondalkar, V. G.: *Organizational Behavior*, New age international limited, New Delhi, 2015., https://www.iibms.org/wp-content/uploads/2015/05/Organizational-Behaviour.pdf, 15.05.2020.
71. Linkov, I., Kott, A.: *Cyber Resilience of Systems and Networks*, preprint version, Springer 2018., https://www.researchgate.net/publication/325680212_Fundamental_Concepts_of_Cyber_Resilience_Introduction_and_Overview
72. Lobova, S.V., Bogovitz, A.V.: *The Subject-Object Identification of Personnel Security Threats*, Espacios, VOL 39 (Num. 24), 2018., https://www.revistaespacios.com/a18v39n24/a18v39n24p34.pdf, 11.05.2020.
73. Љубисављевић, С.: *Организовање и задаци интерне ревизије у домаћим и страним банкама у Републици Србији*, часопис Економски хоризонти, Јануар-април 2013., http://www.horizonti.ekfak.kg.ac.rs/sites/default/files/Casopis/2013_1/SR/Snezana_Ljubisavljevic.pdf, 11.05.2020.
74. Максимовић, Ј.: *Матрица планирања акционих истраживања*, прегледни чланак, Филозофски факултет, Ниш, 2012. година. Доступно на адреси: https://scindeks-clanci.ceon.rs/data/pdf/0353-7129/2012/0353-71291202231M.pdf, 11.05.2020.

75. Матић, В.: *Базелски споразум II*, часопис Банкарство, број 7-8, 2009., https://www.casopisbankarstvo.rs/Portals/0/Casopis/2009/7_8/B07-08-2009-Ekoleks.pdf, 11.05.2020.
76. Миленковић, И.: *Групација светске банке (енгл: World bank Group)*, часопис Економски погледи, број 3/2009, http://www.efpr.edu.rs/Ekonomski%20pogledi/3-2009%20PDF/10.pdf, 11.05.2020.
77. Миловановић, З., Радовановић, Р.: *Информацино-безбедносна култура – императив савременог друштва*, журнал за криминалистику и право БНП, Криминалистичкко-полицијска академија, Београд, 2015.
78. Миљковић, Ј., Шрам (*Schram*), М.: *Организациона субкултура и образовање запослених*, часопис Андрагошке студије, Институт за педагогију и андрагогију, број 1, 2015., http://www.as.edu.rs/search?s=Organizaciona+subkultura+i+obrazovanje+zaposlenih&l=sr, 11.05.2020.
79. Моравчевић, С.: *Цар Душан – гувернер*, дневни лист Вечерње новости, интернет издање, https://www.novosti.rs/dodatni_sadrzaj/clanci.119.html:303780-Car-Dusan---guverner, 11.05.2020.
80. Morcos, M.: *Organisational culture: definitions and trends*, 2018., https://www.researchgate.net/publication/329140215_ORGANISATIONAL_CULTURE_DEFINITIONS_AND_TRENDS, 15.05.2020.
81. Murphy, D.: *A history of information security*, https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/, 11.05.2020.
82. *Највећа крађа идентитета у САД*, http://www.rts.rs/page/stories/sr/story/10/Svet/99601/Najve%C4%87a+kra%C4%91a+identiteta+u+SAD.html, 15.12.2013.
83. Nasir, A. *et al*: *An analysis on the dimensions of information security culture concept: A review*, Journal of Information Security and Applications, Volume 44, February 2019., https://www.sciencedirect.com/science/article/abs/pii/S2214212617306828, 15.05.2020.
84. Огњановић, В.: *Међународна сарадња банкарских политика*, часопис Банкарство, 2005. година, https://www.ubs-asb.com/Portals/0/Casopis/2005/5_6/UBS-Bankarstvo-5-6-2005-Ognjanovic.pdf, 11.05.2020.
85. *Опљачкао банку за милион евра дижући новац са свог рачуна*, http://www.pressonline.rs/info/hronika/291744/opljackao-banku-za-milion-evra-dizuci-novac-sa-svog-racuna.html, 15.12.2013.
86. *Препоруке за безбедност IS CORONA Awarness*, Центар за супервизију информационих система, НБС, 23. март 2020. године, доступно на: https://www.nbs.rs/internet/cirilica/scripts/showContent.html?id=15338&konverzija=no
87. Совиљ, Р., Стојковић-Златановић, С.: *Модели управљања оперативним ризиком у инвестиционим друштвима у процесу европских интеграција Републике Србије*, Институт друштвених наука, Мегатренд ревија, Vol. 15, № 2, 2018: 1-16, 2018. година, https://scindeks-clanci.ceon.rs/data/pdf/1820-3159/2018/1820-31591802001S.pdf, 11.05.2020.
88. Спасојевић Бркић, В.К. *et al.: Димензије организационе културе у мултинационалним предузећима*, часопис Техника, број 69, Београд, 2019., https://scindeks-clanci.ceon.rs/data/pdf/0040-2176/2019/0040-21761902279S.pdf, 15.05.2020.
89. Станишић, М., Радовановић, Д., Лучић, Д.: *Анализа концепта ревизије информационих система према Cobit методологији*, 6. Научни скуп са међународним учешћем Синергија 2010., Универзитет Синергија, Бијељина, Република Српска, https://singipedia.singidunum.ac.rs/izdanje/40521-analiza-koncepta-revizije-informacionih-sistema-prema-cobit-metodologiji, 15.05.2020.

90. Станишић, М.: *Карактеристике модерне ревизије у банкама*, Банкарство 7-8, 2007. године, https://www.ubs-asb.com/Portals/0/Casopis/2007/7_8/UBS-Bankarstvo-7-8-2007-Stanisic.pdf, 11.05.2020.
91. Pahnilaa, S., Siponena, M., Mahmood, A.: *Employees' Behavior towards IS Security Policy Compliance*, 40th Hawaii International Conference on System Sciences, 2007., https://ieeexplore.ieee.org/document/4076692, 11.05.2020.
92. Parsons, K.: *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)*, Somputers & Security, Volume 42, 2014, https://www.sciencedirect.com/science/article/pii/S016740481300179X, 15.05.2020.
93. Ruighaver, A., Maynard, S., Chang, S.: *Organizational security culture: extending the end-user perspective*, Computers & Security, 2007., http://84.205.229.18/securityc/d/english/Culture/Organisational%20security%20culture.pdf, 11.05.2020.
94. Solms, V.B., Solms, V.R.: *The 10 deadly sins of information security management*, Computers & Security, 2004., https://www.uio.no/studier/emner/matnat/ifi/INF3510/v10/learningdocs/VonSolms-10-Deadly-Sins.pdf, 15.05.2020.
95. *Stuxnet* је заразио и једну руксу нуклеарну електрану, тврди директор Kaspersky Lab-a, https://www.informacija.rs/Vesti/Stuxnet-je-zarazio-i-jednu-rusku-nuklearnu-elektranu-tvrdi-direktor-Kaspersky-Lab-a-VIDEO.html, 11.05.2020.
96. Theoharidou M. Gritzalis, D.: *Common body of knowledge for information security*, Security & privacy, IEEE, Видети: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber¼4140992; 2007.
97. *Towards a Conceptual Foundation of Physical Security, Case Study of an IT Department*, Journal of Safety and Security Engineering, Vol. 9, No. 2, 2019., 11.05.2020., https://www.researchgate.net/publication/334516712_Towards_a_conceptual_foundation_for_physical_security_Case_study_of_an_IT_department, 15.05.2020.
98. *Understanding difference between Cyber Security & Information Security - CISO Platform*, https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information?xg_source=activity, 11.05.2020.
99. *Information security culture and information protection culture: A validated assessment instument*, Computer Law & Security Review, Volume 31, 2015., https://www.sciencedirect.com/science/article/abs/pii/S0267364915000060, 15.05.2020.
100. Veigaa, A., Astakhova, Lj. V., Bothac, A., Herelmanc, M.: *Defining organisational information security culture—Perspectives from academia and industry*, Computer & Security, Volume 92, May 2020., https://www.sciencedirect.com/science/article/pii/S0167404820300018?via%3Dihub, 15.05.2020.
101. Велашевић, Д.: *Заштита података у рачунарским системима*, ЈИСА Инфо, год. 4, бр.1, 1996.
102. *Водич кроз информациону безбедност у Републици Србији* , Мисија ОЕБС-а у Србији, Unicom Telecom, IBM, Juniper, Грид студио, Београд, 2018. https://www.osce.org/sr/mission-to-serbia/404258?download=true, 11.05.2020.
103. *Водич кроз информациону безбедност у Републици Србији*, Центар за евроатланске студије – ЦЕАС и Мисија ОЕБС у Србији, Београд, 2016. година, https://www.osce.org/sr/serbia/272206?download=true, 11.05.2020.

104. Вуксановић, Д.: *Стандарди у области безбедности ИКТ*, Институт за стандардизацију Србије, Београд, 2017., доступно на: https://coming.rs/wp-content/uploads/2017/09/Standardi-u-oblasti-bezbednosti-IKT-a.pdf, 11.05.2020.
105. Вулетић Д.: „Шта је информационо ратовање?“, *Безбедност*, бр. 3/05, Београд, 2005, стр. 494.
106. Вулић, И.: *Алармантно стање информационе безбедности у Србији*, http://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:437424-Alarmatno-stanje-informacione-bezbednosti-u-Srbiji, 21.12.2013.
107. Weiner, Y.: *99 Totally Serious Ways To Create A Great Work Culture*, 2018., https://medium.com/thrive-global/99-totally-serious-ways-to-create-a-great-work-culture-e7d093bdad23, 15.05.2020.
108. Wileya, A., McCormac, A., Čalić, D.: *More than individual: Examing the relationchip berween culture and information security Awareness*, Computer & Security, Volume 88, january 2020, https://www.sciencedirect.com/science/article/pii/S0167404819301841, 15.05.2020.
109. Xiaoming, C., Junchen, H.: *A literature Review on Organization Culture and Corporate Performance*, International Journal of Bussiness Administration, Vol. 3, No. 2, 2012., http://www.sciedu.ca/journal/index.php/ijba/article/view/863, 15.05.2020.
110. Шабић, Р.: *Забрињавајуће стање у заштити података*, http://www.blic.rs/Vesti/Drustvo/426048/Sabic-Zabrinjavajuce-stanje-u-oblasti-zastite-podataka, 21.12.2013.
111. Шта је *GDPR*: Права и обавезе корисника интернета, IT Academy, https://www.it-akademija.com/sta-je-gdpr, 11.05.2020.
112. *Улога односа с јавношћу у решавању кризе са леком Tylenol*, http://aleksisdimy.blog.rs/blog/aleksisdimy/generalna/2011/10/12/uloga-odnosa-s-javnoscu-u-resavanju-krize-sa-lekom-tylenol, 11.05.2020.
113. Желесков Ђорић, Ј.: *Резилијентност и задовољство послом хирурга*, Институт за криминолошка и социолошка истраживања, Београд, 2012.

ДОКУМЕНТИ:

114. *Акциони план за 2018. и 2019. годину, за спровођење Стратегије развоја информационе безбедности*, Закључак са седнице Владе, 91. седница Владе Републике Србије, 28. август 2018. Године
115. *Cyber Europe 2018 After Action Report, 2018.*, https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report, 15.05.2020.
116. *Cyber Lexicon*, Financial Stability Board (FSB), 2018., https://www.fsb.org/wp-content/uploads/P121118-1.pdf, 15.05.2020.
117. *Cyber resilience oversight expectations for financial market infrastructures (CROE)*, Europian central bank, 2018.,https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf, 15.05.2020.
118. *Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, O. J. L 176/2013* (Директива о адекватности капитала), *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036*, 17.05.2020.

119. *Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016.*, Official Journal of the European Union L 194/1., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, 11.05.2020.
120. *EU Cybersecurity Act*, 2019., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN, 15.05.2020.
121. *EBA Guidelines on outsourcing arrangements, 2019.*, https://eba.europa.eu/sites/default/documents/files/documents/10180/2761380/78acbfce-18e9-4f4a-8460-717542b3fd34/EBA%20revised%20Guidelines%20on%20outsourcing_HR.pdf, 15.05.2020.
122. *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*, доступно на: https://www.bundesbank.de/resource/blob/764692/01503c2cb8a58e44a862bee170d34545/mL/2018-10-24-g-7-fundamental-elements-for-third-party-cyber-risk-data.pdf, 15.05.2020.
123. *Guidance on cyber resilience for financial market infrastructures*, Bank for International Settlements and International Organization of Securities Commissions, 2016., https://www.bis.org/cpmi/publ/d146.htm, 11.05.2020.
124. *International standard ISO/IEC 27000:2018*, https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip, 15.05.2020.
125. *International standard ISO/IEC* 27002:2005, http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27002.pdf, 15.05.2020.
126. *Joint Advice on the costs and benefits of a coherent cyber resilience testing framework, 2019.*, https://www.esma.europa.eu/sites/default/files/library/jc_2019_25_joint_esas_advice_on_a_coherent_cyber_resilience_testing_framework.pdf, 15.05.2020.
127. *Joint Advice on the need for legislative improvements relating to ICT risk management requirements.* Доступно на: https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf, 15.05.2020.
128. *Кривични законик*, Службени гласник РС, бр. 85/2005, 88/2005, испр. – 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019
129. *Одлука о образовању Тела за координацију послова информационе безбедности*, Службени гласник РС, бр. 24/2016, 53/2017, 79/2017, 112/2017 и 93/2018
130. *Одлука о минималним стандардима управљања информационом системом финансијске институције,* Службени гласник РС, бр. 23/2013, 113/2013, 2/2017 и 88/2019
131. *Одлука о системима управљања и унутрашњих контрола платних институција и институција електронског новца и о заштити новчаних средстава корисника платних услуга и ималаца електронског новца,* Службени гласник РС, бр. 55/2015 и 65/2019
132. *Одлука о управљању ризицима банке,* Службени гласник РС, бр. бр. 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 – др. одлука1 , 43/2013, 92/2013, 33/2015, 61/2015, 103/2016 и 119/2017
133. *Правилник о ближим условима за упис у Евиденцију посебних центара за превенцију безбедносних ризика у информационо-комуникацијским системима*, Службени гласник РС, бр. 12/2017

134. *Принципи за инфраструктуру финансијског тржишта* (енгл: *Principles for Financial Market Infrastructures – PFMI*), *Банка за међународна поравнања (BIS)*, 2012., https://www.bis.org/cpmi/info_pfmi.htm, 11.05.2020.
135. *Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) 648/2012 O. J. L 176/2013* (Уредба о капиталним захтевима), *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0575*, 17.05.2020.
136. *Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. Године*, Службени гласник РС, бр. 53/2017
137. *Стратегија сајбер безбедности ЕУ*, 2013., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001, 11.05.2020.
138. *The European Agenda on Security*, Strasbourg, 2015., https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf, 11.05.2020.
139. *TIBER-EU Framework Services Procurement Guidelines*, European Central Bank, доступно на: https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf, 15.05.2020.
140. *Уредба о начину и поступку означавања тајности података, односно докумената,* Службени гласник РС, бр. 8/11
141. *Уредба о посебним мерама физичко-техничке заштите тајних података Сл. гласник РС, бр. 97/11*
142. *Уредбом о посебним мерама заштите тајних података у информационо-телекомуникационим системима*, Службени гласник РС, бр. 53/11
143. *Уредбом о посебним мерама надзора над поступањем са тајним подацима* , Службени гласник РС, бр. 90/11
144. *Уредбом о посебним мерама заштите тајних података који се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа,* Службени гласник РС, бр. 63/13
145. *Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја*, Службени гласник РС, бр. 94/2016
146. *Уредба о ближем садржају акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедносно-инфорамционог система од посебног значаја,* Службени гласник РС, бр. 94/2016
147. *Уредба о поступку достављања података, листи, врстама и значају инцидента и поступку обавештавања о инцидентима у ИКТ системима од посебног значаја*, Службени гласник РС, бр. 94/2016
148. *Уредбе о поступку достављања података, листи, врстама и значају инцидента и поступку обавештавања о инцидентима у информационо-комуникацијским системима од посебног значаја,* Службени гласник РС, бр. 94/2016
149. *Закон о банкама*, Службени гласник РС, бр. 107/2005, 91/2010 и 14/2015
150. *Закон о Народној банци Србије*, Службени гласник РС, бр. 72/2003, 55/2004, 85/2005 – др. закон, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – одлука УС и 44/2018
151. *Закон о информационој безбедности*, Службени гласник РС, бр. 6/2016, 94/2017 и 77/2019
152. *Закон о тајности података*, Службени гласник РС, бр. 104/2009
153. *Закон о заштити података о личности,* Службени гласник РС, бр. 87/2018
154. *Закон о заштити пословне тајне,* Службени гласник РС, бр. 72/2011
155. *Закон о слободном приступу информацијама од јавног значаја,* Службени гласник РС, бр. 1207/2004, 54/2007, 104/2009 и 36/2010

156. *Законик о кривичном поступку,* Службени гласник РС, бр. 72/2011, 101/2011, 121/2012, 121/2012, 32/2013, 45/2013, 55/2014 и 35/2019
157. *Закон о информационој безбедности,* Службени гласник РС, 2016
158. *Закон о привредним друштвима,* Службени гласник РС, бр. 36/2011, 99/2011, 83/2014 – др.закон, 5/2015, 44/2018, 95/2018 и 91/2019
159. *Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала,* Службени гласник РС, бр. 61/2005, 104/2009

СТАНДАРДИ:

160. *Cobit – Control Objectives for Information and Related Technologies*
161. *GDPR – General Data Protection Regulation*
162. *HIPPA – The Helth Insurance Portability and Accountability Act*
163. ISO 17799
164. ISO/IEC 27001
165. ISO/IEC 27002
166. ISO 31000
167. *NIST 800-16 – Information Technology Security Training Requirements: A Role- and Performance-Based Model*
168. *PCI DSS – The Payment Card Industry Data Security Standard*

VII ПРИЛОЗИ

Прилог 1

Изјава о ауторству

Име и презиме аутора _____

Број индекса _____

Изјављујем

да је докторска дисертација под насловом

_____

_____

- резултат сопственог истраживачког рада,
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио ауторска права и користио интелектуалну својину других лица.

Прилог 2

Изјава о истоветности штампане и електронске верзије

докторског рада

Име и презиме аутора _____

Број индекса _____

Студијски програм _____

Наслов рада _____

_____

Ментор _____

Потписани _____

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао ради похрањивања у Дигиталном репозиторијуму Универзитета у Београду. Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада. Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

У Београду, Потпис аутора

_____ _____

Прилог 3

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић” да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

_____

_____

која је моје ауторско дело.

Дисертацију са свим прилозима предао сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио.

1. Ауторство (CC BY)
2. Ауторство – некомерцијално (CC BY-NC)
3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)
4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)
5. Ауторство – без прерада (CC BY-ND)
6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

У Београду, Потпис аутора

_____ _____