УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

СТАНДАРД ISO 27001:
УПРАВЉАЊЕ БЕЗБЕДНОШЋУ ИНФОРМАЦИЈА

ДИПЛОМСКИ РАД

МЕНТОР:

Проф. др Зоран Драгишић

КАНДИДАТ:

Милена Перић 127/14

Београд, 2020.

САДРЖАЈ

УВОД

У модерном радном окружењу, заштита и безбедност информација имају све већи значај, а обзиром да смо сведоци наглог развоја и употребе информационих технологија у свим организационим токовима. За организације, информације представљају кључне ресурсе, те је њихова заштита од виталног значаја. Осигурање безбедности информација, заправо, представља чување информација као „знања“ организација, а које представља суштински ресурс за данашње системе менаџмента. У правцу остварења безбедности информација, усвојен је стандард ISO 27001 у којем су специфирани захтеви које организација треба да поштује да би остварила систем за заштиту информација.

Увођењем овог стандарда омогућава се унапређење заштите информација кроз дефинисану поверљивост, интегритет и приступ информацијама. Да би, у данашњем пословном окружењу, организације могле да испуне бројне захтеве који се намећу њиховим системима менаџмента безбедношћу (па тако и менаџмента безбедношћу информација), оне морају да у своје пословање интегришу различите међународне стандарде. За овај рад значајни су стандарди серије ISO/IEC 27000, донети од стране Међународне организације за стандардизацију (ISO) и Међународне електротехничке комиције (IEC). Сврха ових међународних стандарда је да пруже помоћ организацијама свих врста и величина да развију и примене системе за управљање безбедношћу сопствених информација, као и да се припреме за независно и непристрасно оцењивање (сертификацију) тог система. Овај систем примењује се за заштиту информација као што су, на пример, финансијске информације, информације о интелектуалној својини, подаци о особљу или информације које су организацији поверене од корисника или треће стране (Живковић, Крњајић, 2009).

Предмет овог рада односи се на опис основних карактеристика, захтева, приступа и предности увођења стандарда ISO 27001 за управљање безбедношћу информација, а који представља саставни део серије стандарда ISO/IEC 27000. Циљ је да се укаже на значај који имплементација овог стандарда у системе менаџмента има за укупно пословање, раст и развој организација у модерном пословном окружењу.

1. БЕЗБЕДНОСТ ИНФОРМАЦИЈА - појам и значај

Данашње пословање незамисливо је без примене информационих технологија. Информације представљају веома важан ресурс од кога зависи опстанак и развој организација. Организације су данас све отвореније, повезујући своје информационе ресурсе са купцима, добављачима и слично. Међутим, таква транспарентност информација доводи и до појаве бројних претњи по њихову сигурност. Данашњи безбедносни изазови у вези са информацијама односе се на рачунарске преваре, шпијунаже, саботаже, хаковања итд. Овакве појаве могу умногоме наштетити пословању једног предузећа и зато је врло важно да се информације, без обзира у ком су облику, адекватно заштите. У савременом пословању, тако, заштита информација постаје задатак који је од примарне важности (Ђапић, Лукић, 2007).

1.1. Појам информација

Информације представљају главне одлике информационих технологија, знања и друштва. Најпростије речено, информација се може дефинисати као порука која је примљена и схваћена. Информација представља резултат организовања података, процесуирања података, као и манипулисања подацима. Сви ови процеси обављају се на начине да се надогради знање особе која прима информацију. Дакле, информацијом се доноси ново сазнање за њеног примаоца (Латиновић, Рољић, 2014). Информација је, дакле, „податак са одређеним значењем, односно знање које се може пренети на било који начин (писмом, аудио, визуелно, електронски или на неки други начин). Информације могу да буду: штампане или написане на папиру; одложене (меморисане) електронски; пренесене поштом или електронским путем; приказане на корпорацијском веб сајту; вербалне - изговорене у конверзацији“ (Ђапић, Лукић, 2007).

Информација има неколико основних обележја:

- *релевантност* - повезује са са релевантношћу догађаја на који се односи информација или релевантношћу догађаја за одређеног корисника; релевантне

информације су потпуне, тачне, разумљиве, док то није случај са информацијама о неком свакодневном догађају;

- *потпуност* - догађај је потребно довољно описати; ипак сваки догађај не може бити описан у потпуности и посматрано из сваког угла, па је зато потребно на почетку дефинисати оквир описа догађаја (време, место, начин дешавања, итд.); непотпуна информација се допуњава претходним и накнадним информацијама о догађају, принципима и законима који нису наведени јер се подразумевају и претпоставкама;
- *репрезентативност* - описује репрезентативне карактеристике догађаја;
- *тачност* - подударност информације и догађаја, у складу са могућностима посматрача и потребама корисника информација;
- *разумљивост* - једноставно и недвосмислено тумачење; даваоц информације треба да разумљиво опише догађај и да постоји потреба корисника да разуме информацију, како би стекао реалну слику догађаја;
- *правовременост* - односи се на временске интервале од дешавања неке ситуације до састављања и дистрибуције информације; потребно је добити информацију у правом тренутку;
- *поверљивост* - односи се на поверљивост догађаја који се описује; овим информацијама приступ имају само особе које за то имају одговарајућа овлашћења (Латиновић, Рољић, 2014).

За овај рад посебно су значајне пословне информације, односно све информације које су у функцији делатности пословног субјекта, односно информације потребне за његово пословање и остваривање пословних циљева и интереса. Пословне информације, а да би биле употребљиве и имале одређени значај за организацију, морају да задовоље неколико основних начела: оне морају да буду правовремене, објективне, тачне, проверене, потпуне, поуздане и заштићене. Наиме, да би један пословни субјект могао пословну информацију да експлоатише и да њеном спознајом постигне очекивани пословни резултат, она мора да буде обезбеђена у повољном тренутку, односно да буде *правовремена*. Важно је и да информација буде *објективна* - да би информација имала

вредност и важност за пословног субјекта, она мора да буде посматрана непристрасним очима корисника. Ово је једно од најкомплекснијих пословних начела, јер је веома тешко искључити субјективне факторе (попут животних искустава, образовања, окружења итд.) приликом доношења пословних одлука. Због необјективности, оргнанизације често праве грешке у свом пословању, и зато је врло важно да информације које се користе у пословању буду што објективније (Протић, 2013).

Пословна информација треба да буде и тачна. *Тачност* информације у поступку доношења одлука има посебну важност за организацију. Наиме, само на основу тачних информација, организација може да доноси квалитетне одлуке, те се због тога овом начелу посвећује посебна пажња. Информације треба да буду и *проверене* - без обзира са колико вероватноћом може да се тврди да је нека информација тачна, уколико не постоји могућност за проверу из других извора, она се узима са резервом. Информација која може да се провери из више извора, има већу важност за организацију. *Потпуност* је још једно од начела које треба да задовољи информација а да би имала вредност за организацију. Наиме, пословна информација може да буде тачна и проверена, али ако није потпуна, она нема одговарајућу важност за организацију и не обезбеђује јој доношење квалитетних информација. Да би информација била потпуна, она мора да поседује све елементе и да буде „заокружена“ тако да доносиоцу одлука обезбеди недвосмислену предност у односу на конкурента и минимални пословни ризик (Протић, 2013).

Следеће начело је *поузданост*. Ово начело одређено је претходним начелима - информација не може да буде поуздана ако није тачна, односно не може да буде поуздана ако није проверена из више извора. И на крају, информација мора да буде *безбедна и заштићена*. Основни задатак сваке организације представља заштита и обезбеђење осетљивх пословних информација, односно спречавање неовлашћеним лицима да им приступе (Протић, 2013). Колико је значајно заштитити информације, видећемо у даљем тексту.

1.2. Појам и значај безбедности информација

Концепт безбедности информација има за циљ да одреди смернице за заштиту информација, информационе имовине и информационог система. Како информација у данашњим условима пословања представља највреднији капитал организације, врло је важно применити и адекватне политике и процедуре како би се исте заштитиле од различитих фактора угрожавања. "Информације и њима припадајући подаци, затим процеси и системи (хардверски, софтверски, мрежни итд.) који се користе за њихово генерисање, обраду, пренос, меморисање као и приступ представљају важан део пословне имовине организације коју је потребно прикладно заштитити ако се жели нормално пословање које ће обезбедити опстанак и развој. Овај захтев постаје све важнији због дистрибуиране пословне околине организације у којој су информације изложене рањивостима услед великог броја претњи (опасности)" (Ђапић, Лукић, 2007).

На Табели 1. приказане су категорије информационих ресурса које је потребно заштитити.

Табела 1. Категорије информационих ресурса које је потребно заштитити

Категорија информационих ресурса (вредности)	Примери
Информације	Базе података и подаци, документа везана за систем, кориснички приручници, материјали за обуку, оперативне и системске процедуре, систем записа
Софтвер	Апликативни и системски софтвер, алати за развој софтвера
Физички ресурси - хардвер (компјутерска опрема)	Компјутерски уређаји (процесори, монитори, лаптопови), комуникациони уређаји (рутери, свичеви, телефони), магнетни медијуми (траке, дискови), остали технички уређаји
Услуге	Услуге обраде података, комуникационе услуге
Особље	Знање и вештине особља (техничког, оперативног, маркетинг, финансијског итд.)

Извор: Ђапић, Лукић, 2007

Информациони ресурси, споменути у Табели изнад, независно од врсте и природе, морају се заштитити јер су исти: препознати на нивоу организације као ентитет који има

вредност; не могу лако да буду замењени без утрошка ресурса (новца, вештине запослених, времена итд.); чине идентитет организације без кога пословање организације може да буде угрожено (Ђапић, Лукић, 2007).

Информациони ресурси могу да буду угрожени деловањем различитих фактора. Претње могу долазити од: запослених, ниске свести о потреби заштите информација (корпоративна култура), пораста умрежености и дистрибуиране обраде података, пораста сложености и ефективности хакерских алата и вируса, е-маил-ова, пожара, поплава, земљотреса итд. Без обзира на извор претње, основни циљеви заштите информација у некој организацији су: обезбеђивање континуитета пословања и минимизација ризика од потенцијалних штета (хаварија). Ово се постиже, пре свега, превенцијом штетних догађаја и смањењем њиховог потенцијалног утицаја. Од пресудне важности може бити и дефинисање, имплементација, одржавање и унапређење концепта и стандарда безбедности информација (Атанасијевић, 2009).

Информације које за организације имају велику вредност, угрожене су, дакле, великим бројем различитих претњи и извора угрожавања. Свака организација тежи да заштити своје информације, и за то тражи јединствено решење. Како су информациони ресурси комплексни и многобројни (свака организација садржи мноштво информација и података, поверљивих и оних са мањим степеном поверљивости), прави је изазов очувати потребан ниво безбедности. Сасвим је јасно да се изазови и ризици не могу у потпуности елиминисати, али се исти могу предвидети и планирати, те се на њих може превентивно деловати, односно створити систем заштите који ће управљати њима, кроз активан одговор на претње. У том погледу, потребно је имплементирати сигурносне мере и процедуре у циљу: одвраћања, превенције, детекције и оправке од утицаја догађаја који делују на кључна обележја пословних информација.

2. СТАНДАРДИЗАЦИЈА У ОБЛАСТИ (БЕЗБЕДНОСНОГ) МЕНАЏМЕНТА ОД ЗНАЧАЈА ЗА БЕЗБЕДНОСТ ИНФОРМАЦИЈА

Заштита информација представља кључ за успех данашњих организација. Она се постиже применом различитих мера и поступака, односно техничких решења. Али, она је и много више од тога. Ако пођемо од тврдње аутора Кенинга, М. „Ако мислите да технологијом можете решити ваш сигурносни проблем онда ви не разумете ни проблем ни технологију“ (Kenning, 2001), уочићемо да концепт безбедности информација представља много више од примене савремених техничких решења које нуде информационе технологије. Наиме, заштита безбедности информација остварује се, поред примене ових техничких решења, и имплементацијом одређених стандарда развијених од стране међународних организација за стандардизацију.

Стандарди у области безбедносног менаџмента развијени су како би описали скуп процедура које једна организација треба да следи, а како би опстала и развијала се на конкурентном и динамичном тржишту. У зависности од специфичности организације, систем менаџмента може обухватити различите системе, као шти су систем менаџмента квалитетом, систем менаџмента животном средином, систем менаџмента заштитом здравља и безбедности на раду, па и систем менаџмента безбедности информација. За сваки од ових система постоје и одређени стандарди којих свака организација мора да се придржава а како би достигла постављене циљеве. Сваки развијени стандард фокусира се на једну димензију пословања, а међусобно су компатибилни (Драгишић, Радојевић, 2014).

Савремено пословање карактерише се интензивним променама, јаком конкуренцијом и бројним ризицима и све различитијим захтевима из области ефикасности и ефективности пословања, конкурентности, одрживог развоја, друштвено одговорног пословања итд. Ове захтеве тржишта и различите ризике пословања, организација може да реши системским приступом, односно усклађивањем са захтевима одговарајућих међународних управљачких стандарда. Ови управљачки стандарди примењују се на све

системе у једној организацији, па тако и на систем безбедности (Вујичић, Станковић, 2011).

2.1. Појам и значај стандарда

У документима међународних организација, стандард се дефинише као документ којим се утврђују захтеви, спецификације, правила, смернице или карактеристике које треба конзистентно следити и испунити да би се обезбедило да материјал, производи, процеси, услуге, заиста могу служити за њихову основну намену. Стандарди треба да се заснивају на провереним резултатима науке, технологије и искуства, а ради постизања оптималне користи за друштво (Драгишић, Радојевић, 2014).

Стандарди позитивно утичу на све аспекте пословања. Они увек представљају проверена решења, те коришћење стандардних решења у највећој могућој мери доприноси ефикасности развојних активности, уз одговарајуће смањење ризика од непожељних ситуација. У пракси, стандард заштите садржи читав сет аранжмана за покривање што већег броја типичних безбедносних захтева за одржавање ризика на прихватљивом нивоу. Стандарди заштите обезбеђују препоруке за развој, имплементацију и одржавање система заштите главни су алат за побољшање квалитета контрола заштите интегрисањем делова стандарда у све пословне процесе. Основна обележја сваког стандарда су: документованост, расположивост, свеобухватност, да је издат од стране националног тела за стандардизацију, адекватан намени, рентабилан, добровољно прихваћен, усаглашен са законима и да обезбеђује индикаторе прогреса (Грубор, Милосављевић, 2010).

Према Грубору (2010), општи модел стандарда заштите укључује следеће елементе:

- *терминологија* - укључује листу дефиниција и појмова;
- *принципи* - обезбеђују аксиоматска правила за израду упутства заштите;
- *методологија* - обезбеђује поједностављен опис начина коришћења концепта, метода и техника, као и њихових међусобних односа;
- *елементи стандарда* - обезбеђују специфичне захтеве за дефинисану компоненту заштите;

- *упутство и додаци за примену* - обезбеђују детаљан опис примене елемената стандарда у специфичним ситуацијама;
- *технике и алати* - подржавају примену стандарда (Грубор, Милосављевић, 2010).

Значај примене стандарда указан је и у нашем Закону о стандардизацији[1], којим се уређују циљеви и начела стандардизације у Србији, организовање и делатност националног тела за стандардизацију, као и доношење, објављивање и примена српских стандарда и сродних докумената. У члану 5. овог закона као циљеви стандардизације дефинисани су следећи:

1) унапређење заштите живота, здравља и безбедности људи, животиња и биљака, као и заштите животне средине;
2) побољшање квалитета производа, процеса и услуга, њихова типизација, компатибилност и заменљивост;
3) обезбеђење јединствене техничке основе;
4) развој и унапређивање производње и промета производа, извођења радова, односно вршења услуга кроз развој међународно усклађених стандарда ради ефикасног коришћења рада, материјала и енергије;
5) унапређење међународне трговине, спречавањем или отклањањем непотребних техничких препрека.

2.1. Међународни стандарди за заштиту безбедности информација

У области заштите информација, постоје бројна међународна тела која се баве стандардизацијом. Кључне организације су: ISO (енг. *International Organization for Standardisation*), BSI (енг. *British Standards Institute*), BSI (нем. *Bundesamt fuer Sicherheit in der Informationstechnik*, German), IEC (енг. *International Elektrotechical Commision*), NIST (енг. *National Institute for Standards and Technology*, USA). Стандарде заштите информација доноси Међународни технички комитет за стандардизацију ISO/IEC JTC1/

[1] *Закон о стандардизацији*. „Службени гласник РС“, бр. 36/2009 и 46/2015.

SC27, формиран 1990. године, а који се састоји од следећих тела: 1) систем за управљање заштитом информација; 2) криптографски и други механизми заштите; 3) критеријуми за евалуацију заштите; 4) сервиси и контроле заштите; 5) технологије за заштиту приватности и управљање идентитетом (Грубор, Милосављевић, 2010).

Постоји више стандарда (тачније 6) који се односе на поље информација, комуникација и безбедности информација. Ни један од њих не покрива све области у којима је потребна заштита података, већ се они међусобно допуњују и тако регулишу компленту област информационо-комуникационог система. Следећи су стандарди у области безбедности информација: ISO/IEC 15408 за интеграцију захтева за безбедност у софтверским процесима, спецификацију карактеристика производа и проверу испуњености захтева за информациону безбедност; ISO/IEC 113335 за управљање безбедношћу информационих технологија; ISO/IEC 17799 стандард за информациону безбедност који је еволуираоу у стандарде ISO/IEC 27000 за прављење система заштите информација и стандард NIST SP 800 (Грубор, Милосављевић, 2010).

Стандардизација у оквиру система заштите информација производи бројне предности за организацију:

- смањење комплексности управљања системом заштите;
- већа могућност извора и израда стандардне документације;
- обезбеђење интероперабилности различитих система заштите;
- формирање базе знања у области заштите;
- незаменљиви алат у процесима сертификације и акредитације система заштите;
- обезбеђује осетљиве методе и дефинише најбољу праксу заштите (Грубор, Милосављевић, 2010).

За овај рад, од посебног значаја су стандарди из серије ISO/IEC 27000, тачније стандард 27001. О овом стандарду, више речи у наредном поглављу.

3. СТАНДАРД ISO 27001 - заштита безбедности информација

Као што је већ напоменуто, заштита и безбедност информација у данашњем пословном свету од великог је значаја. Савремено пословање у великој мери зависи од информационих технологија, комуникација путем мрежа, као и бежичних и мобилних комуникација. Како се све чешћи видови савременог пословања односе на обављање послова путем интернета и компјутера, тако је постало све важније адекватно заштитити ове информације од различитих компјутерских превара, односно безбедносних ризика. Успешно пословање и доношење добрих одлука могуће је остварити само уз правовремени приступ правим и сигурним информацијама које су за то неопходне. Заштита таквих информација постаје предуслов за остваривање претходно поменутог и зато је потребно прићи систематски тој материји (Живковић, Крњајић, 2009).

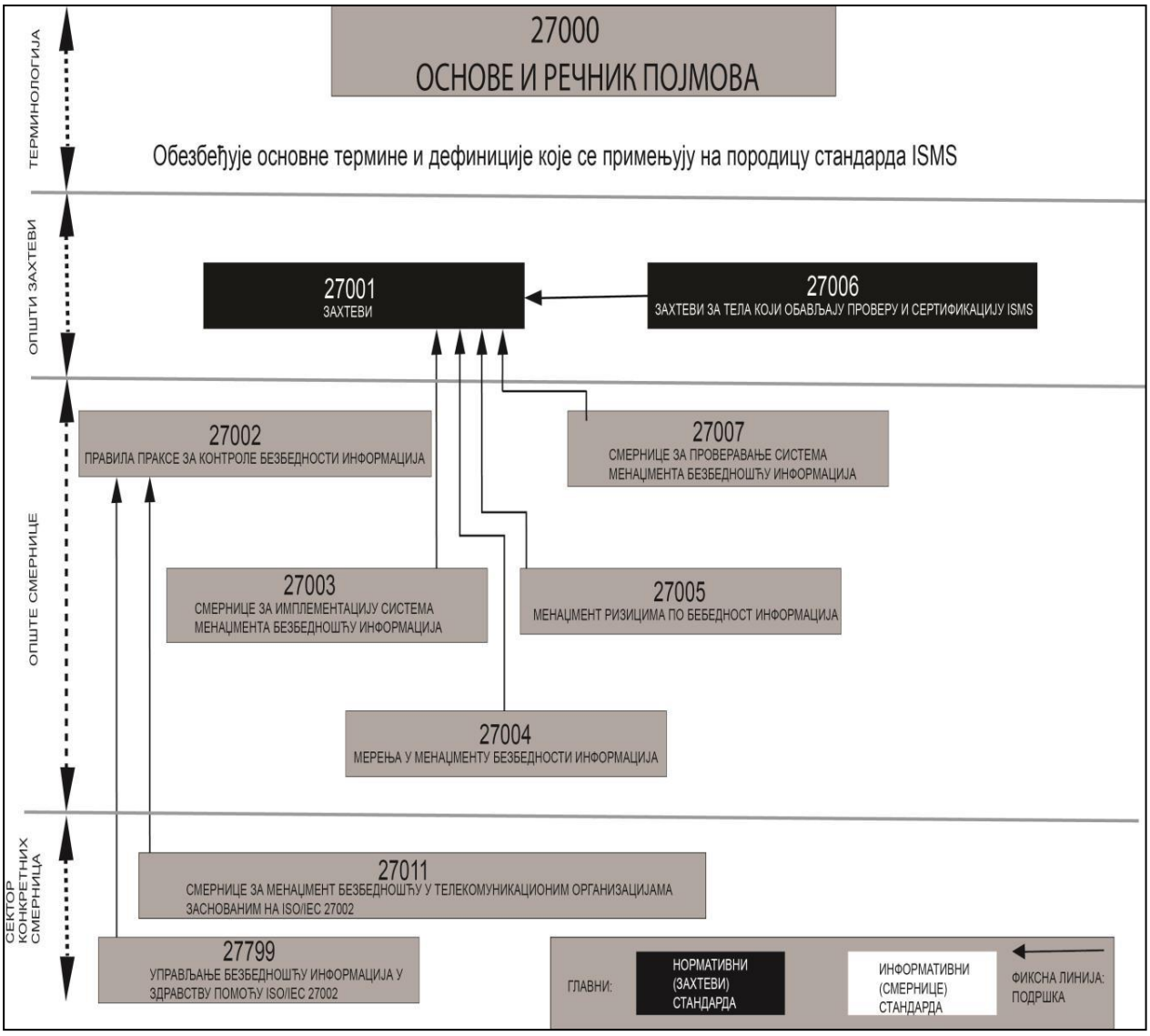
Један од начина да се свеобухватним приступом заштите информације у пословању јесте интеграција међународних стандарда. У том смислу, посебно су значајни међународни стандарди серије ISO/IEC 27000, који се односе на информационе технологије, технике заштите и систем менаџмента безбедношћу информација. У овом делу рада, најпре ће бити речи уопштено о породици стандарда 27000, а потом ће детаљна пажња бити посвећена стандарду 27001, који је и предмет овог рада.

3.1. Стандарди серије ISO/IEC 27000

Стандарди серије ISO/IEC 27000- *Систем управљања безбедности информација*, донети су од стране Међународне организације за стандардизацију (ISO) и Међународне електротехничке комисије (IEC). Сврха ових међународних стандарда је да пруже помоћ организацијама свих врста и величина и да развију и примене систем за управљање безбедношћу сопствених информација, као и да се припреме за независно и непристрасно оцењивање (сертификацију) тог система. Овај систем примењује се за заштиту информација као што су, на пример, финансијске информације, информације о интелектуалној својини, подаци о особљу или информације које су организацији поверене од корисника или треће стране (Живковић, Крњајић, 2009).

Основни стандарди који припадају породици стандарда ISO/IEC 27000 приказани су на слици испод.

Слика 1. Серија стандарда ISO/IEC 27000



Извор: ISO/IEC, 2018

Ова серија стандарда обухвата стандарде који дефинишу захтеве за систем менаџмента безбедности информација (енг. скраћ. ISMS), као и захтеве за тела која сертификују ISMS; обезбеђују подршку, детаљна упутства и инструкције за целокупан процес успостављања овог система; дају специфична секторска упутства за ISMS и оцењивање усаглашености са ISMS. Серија стандарда ISO/IEC 27000 у вези је са многим

другим ISO и ISO/IEC стандардима који се односе на област безбедности информација и који обезбеђују специфичне захтеве, упутства и слично.

3.2. Стандард 27001

Стандард ISO/IEC 27001 је део растуће ISO/IEC 27000 серије стандарда, донет од стране међународне организације за стандардизацију (ISO) и Међународне електротехничке комисије (IEC), октобра 2005. године. Пун назив овог стандарда је: ISO/IEC 27001: 2005 - информациона технологија - сигурносне технике - информације о безбедности сигурносне технике - информације о безбедности управљања системима - захтеви, али уобичајено је познат као ISO 27001. Овај стандард намењен је за управљање безбедношћу информација. Захтеви стандарда воде ка креирању система менаџмента безбедности информација (ISMS), чији је циљ управљање безбедношћу информација, а тиме и безбедношћу целе организације (Живковић, Крњајић, 2009).

ISO 27001 настаје као последица потребе дефинисања међународно прихваћених норми, који ће својим захтевима дефинисати оквир формирања свеобухватних система заштите и циљеве његовог деловања, а како би се на ефективан и ефикасан начин управљало безбедношћу информација. Овај стандард својим захтевима дефинише четири главна подручја система заштите информација: 1) систем менаџмента безбедности информација, 2) одговорност руководства, 3) оцена руководства, 4) унапређење ISMS-а (Ђапић, Лукић, 2007).

ISO 27001 је свеобухватан јер третира безбедност информација са три аспекта:

1) *информатичког* - анализирајући и дефинишући перформансе ИТ опреме, права приступа, криптовања, лозинке, протоколе, политике са аспекте појаве ризика по безбедност података и информација;
2) *административног* - дефинишући јасна упутства, политике и процедуре за генерисање информација, њихову дистрибуцију, чување (складиштење);
3) *физичког* - физичка контрола приступа, евиденција запослених, видео надзор, заштита радних просторија итд (ISO, 2013).

Узимајући у обзир сва три аспекта, ISO 27001 дефинише оквир за креирање ISMS који је конципиран тако да пружи потпуну информатичко-физичко-техничку заштиту информација. Систем менаџмента безбедности информација (ISMS), а према захтевима овог стандарда, постаје део укупног система организације, а има за циљ да успостави, имплементира, делује, надгледа, прегледа, одржава и унапређује безбедност информација узимајући у обзир све ризике по пословање организације (ISO, 2013).

Систем менаџмента за безбедност информација (ISMS) покрива следећа подручја:

- анализа и управљање ризиком;
- политика безбедности;
- безбедност организације;
- класификација и управљање имовином;
- политика безбедности у управљању људским ресурсима;
- физичка и информатичка безбедност имовине и окружења организације;
- управљање комуникацијама и оперативом;
- контрола приступа;
- развој и одржавање система;
- управљање инцидентима;
- управљање континуитетом пословања кроз побољшања;
- усаглашеност за законским прописима (Живковић, 2012).

Стандард ISO 27001 у потпуности подржава општеприхваћени концепт да се сигурност информација постиже применом различитих мера заштите података од губитака њихове: 1) *поверљивости* - односи се на заштиту одређених података, односно информација од било каквог намерног или ненамерног откривања неовлашћеним особама; 2) *целовитости (интегритета)* - односи се на осигурање тачности и целовитости информација и на онемогућавање неовлашћене промене њиховог садржаја; 3) *расположивости* - односи се на то да су релевантне информације у временски прихватљивим терминима расположиве одговарајућим субјектима (Живковић, Крњајић, 2009).

3.2.1. Значај стандарда

Стандард ISO 27001 се примењује у различитим подручјима, а у циљу разликовања могућих процеса у организацији који су повезани са управљањем контролом сигурности као што су: политика сигурности, сигурност организације, контрола и класификација извора, сигурност особља, сигурност материјалних добара и животне средине, оперативно управљање и комуникација, контрола приступа, развој и одржавање разних система и управљање континуитетом пословања. Овај стандард је од посебног значаја јер његовим увођењем у системе безбедности, односно системе менаџмента, организације стичу бројне предности и користи.

Користи и предности примене овог стандарда могу се поделити у два дела (два сегмента):

1) заштита и безбедност информација организације и
2) заштита и безбедност података и информација клијената (ISO, 2013).

Први сегмент значи да се увођењем овог стандарда, штите организационе (пословне) информације, а тиме и знање организације и то кроз систематски и проактивни приступ за идентификовање и борбу против читавог низа потенцијалних ризика којима су изложене информације организације. Управљајући ризиком по безбедност информација, смањује се вероватноћа појаве непредвиђених ситуација (претњи) на минимум. *Други сегмент* се односи на заштиту и безбедност података и информација клијената са којима организација долази у контакт приликом инсталирања опреме, извођења обука, пројектовања и монтаже уређаја итд. Овај сегмент представља компететивну предност организације над конкуренцијом, не само приликом добијања квалитетних послова, већ и приликом избора организације као потенцијално поузданог партнера (ISO, 2013).

Организације које поседују сертификат о систему управљања безбедношћу информација који је имплементиран у складу са захтевима стандарда ISO 27001, стичу конкурентну предност на тржишту јер оне на тај начин пружају својим клијентима доказ да ће њихове информације, као и знање организације са којима дата организација долази у

контакт, бити безбедни и заштићени од злоупотреба. Уједно се овим повећава и поверење у дату организацију.

Још неке од користи које организације добијају применом система менаџмента безбедношћу информација (ISMS) и његовом сертификацијом сагласно захтевима ISO 27001 су:

- *just-in-time* ефекат - права информација на правом месту у право време;
- заштита и очување компанијског знања;
- повећање ефективности и ефикасности информационог система;
- повећање пословног кредибилитета и поверења од стране клијената и партнера;
- продор на захтевно међународно тржиште;
- могућност дугорочног интересног умрежавања са другим компанијама;
- уштеда времена рационализацијом количине и садржине информација;
- оптимизација ресурса потребних за дистрибуцију и чување података;
- смањење неспоразума код запослених услед укрштања информација;
- обезбеђивање јасног протока и расположивости информација итд (Вулетић, 2011).

Стандард ISO 27001 намењен је свим оним компанијама и предузећима које се баве услугама које су повезане са информационом технологијом и зато имају потребе за очување поверљивих информација. Коришћењем овог стандарда, компанија доказује својим корисницима или клијентима да послује одговорно и да стално унапређује систем менаџмента за безбедност информација. И управо у томе се огледа велики значај који има примена овог стандарда.

Увођење стандарда из серије ISO 27000 у системе организације, представља унапређење за организацију јер постојање ефективног система управљања безбедношћу информација олакшава организацији следеће: стицање поверења корисника, нарочито ако посао захтева употребу поверљивих информација у власништву корисника (што уопште није редак случај: банке, лабораторије, развој хардвера и/или софтвера и база података,

услужно чување добара, технологија производње и пружања услуга итд.); контролу над ризицима нарушавања безбедности сопствених поверљивих информација; и предност при добијању послова који подразумевају рад са поверљивим информацијама. Изграђивање система управљања безбедношћу информација требало би да пружи могућност заштите људи и информација, те постави нова правила понашања свих корисника информационих ресурса.

3.2.2. Захтеви стандарда

Стандард, осим што пружа бројне предности и користи за организације, производи и одређене захтеве које организација мора да испуни. Наиме, свака организација мора најпре да утврди спољна и унутрашња питања која су релевантна за њену сврху и која утичу на њену способност да оствари жељени резултат свог система менаџмента безбедности информација. Такође, организација мора да утврди заинтересоване стране које су релевантне за систем менаџмента безбедношћу информација и захтеве тих заинтересованих страна који су релевантни за безбедност информација[2]. Организација мора још да одреди границе и применљивост система менаџмента безбедношћу информација, а како би утврдила предмет и подручје његове примене.

Највише руководство мора да покаже лидерство и посвећеност у односу на систем менаџмента безбедношћу информација тиме што:

- обезбеђује да су политике и циљеви система менаџмента безбедношћу информација успостављени и да су компатибилни са стратешким правцем организације;
- обезбеђује интегрисање захтева система менаџмента безбедношћу информација у процесе организације;
- обезбеђује расположивост ресурса потребних за систем менаџмента безбедношћу информација;

[2] Види више на: https://www.kvalitet.org.rs/infrastruktura/standardi/iso-27001-i-iso-22301, приступљено: 10.08.2020.

- саопштава значај ефективног система менаџмента безбедношћу информацциja и усаглашености са захтевима система менаџмента безбедношћу информација;
- обезбеђује да систем менаџмента безбедношћу информација достиже свој планирани резултат (резултате);
- усмерава и подржава остале да доприносе ефикасности система менаџмента безбедношћу информација;
- промовише стално побољшање;
- подржава друге релеватне руководеће улоге да покажу своје лидерство и посвећеност на начин који одговара областима њихових одговорности (Живковић, Крњајић, 2009).

Према захтевима стандарда, политика безбедности мора да буде: доступна као документована информација; саопштена у оквиру организације и доступна заинтересованим странама, у зависности од потребе (ISO, 2013) . Највише руководство мора да осигура да су одговорности и овлашћења за релевантне улоге додељени и саопштени у организацији. Највиши ниво менаџмента мора да додели одговорности и овлашћења за обезбеђење да је систем менаџмента безбедношћу информација усаглашен са захтевима овог међународног стандарда. Организација, још, мора да планира мере које се односе на ризике по безбедност информација, како да те мере интегрише у своје процесе система менаџмента безбедношћу информација, односно како да их примени и вреднује њихову ефективност.

Стандард захтева још и да организације обавезно дефинишу и примене процес оцењивања ризика по безбедност информација. Овај процес:

- успоставља и одржава критеријуме за ризик по безбедност информација који обухватају: критеријуме за прихватање ризика и критеријуме за оцењивање ризика по безбедност информација;
- обезбеђује да поновљено оцењивање ризика по безбедност информација производи конзистентне, валидне и упоредиве резултате;

- идентификује ризике по безбедност информација: примењује процес оцењивања ризика по безбедност информација да би се идентификовали ризици повезани са губитком поверљивости, интегритета и расположивости информација унутар подручја примене система менаџмента безбедношћу информација и идентификује власнике ризика;
- анализира ризике по безбедност информација: оцењује потенцијалне последице уколико се ризици остваре, оцењује реалну вероватноћу појаве ризика и утврђује нивое ризика;
- вреднује ризике по безбедност информација: упоређује резултате анализа ризика са критеријумима за ризик и одређује приоритет међу анализираним ризицима за поступање са њима (ISO, 2013).

Циљеви безбедности информација морају да буду: конзистентни са политиком безбедности информација; буду мерљиви; узимају у обзир применљиве захтеве за безбедност информација и резултате процене ризика и поступања са ризиком; морају да се ажурирају по потреби. Организација мора да чува документоване информације о циљевима безбедности информација.

Приликом планирања како да оствари наведене циљеве безбедности информација, организација мора да утврди:

- шта ће да се уради,
- који ресурси ће бити потребни,
- ко ће бити одговоран,
- када ће то да буде завршено,
- како ће се вредновати резултати (ISO, 2013).

Захтеви стандарда ISO 27001 налажу још да организација мора да утврди потребе за интерним и екстерним комуницирањем које је од значаја за ISMS, где притом треба да узме у обзир следеће: о чему ће комуницирати, када ће се комуницирати, са ким ће се комуницирари, ко сме да комуницира, процесе којима ће се вршити комуникација. Систем

менаџмента безбедношћу информација мора да обухвати документоване информације које захтева овај стандард, односно документоване информације које је организација утврдила као неопходне за ефективност система управљања безбедношћу информација. Приликом креирања и ажурирања документованих информација, организација мора да обезбеди следеће: идентификацију и опис (нпр. наслов, датум, аутора или број на који се позива), формат (нпр. језик, верзија софтвера, графике), медијум (нпр. папирни, електронски) и преиспитивање и одобравање прикладности и адекватности.

Према захтевима овог међународног стандарда, организација обавезно мора да усвоји и план поступања са ризиком по безбедност информација и о томе да чува документоване податке. Организација мора да вреднује перформансе безбедности информација и ефективност система менаџмента безбедношу информација. Уз то, потребно је да организација спроводи интерне провере у планираним интервалима, а ради обезбеђивања информација о томе да ли је систем усаглашен са сопственим захтевима организације за ISMS као и са захтевима овог међународног стандарда, односно да ли је ефективно примењен и одржаван (ISO, 2013).

Преиспитивање ISMS у планираним интервалима значајно је и да би се осигурала стална прикладност, адекватност и ефективност. На основу процена и провера, могуће је спровођење корективних мера, а које морају да буду сразмерне ефектима које су проузроковале настале неусаглашености. О свим предузетим мерама организација мора да чува документоване податке а као доказ о природи неусаглашености и резултатима сваке корективне мере. Стандард ISO 27001 захтева од организација да стално побољшавају прикладност, адекватност и ефективност система менаџмента безбедношћу информација (ISO, 2013).

На основу свега наведеног, може се закључити да, при увођењу стандарда ISO 27001, организација треба да: 1) систематски процењује ризике по информациону безбедност; 2) осмисли свеобухватан пакет контрола информационе безбедности; 3) усвоји свеобухваран поступак управљања, а како би осигурали континуитет у примени мера информационе безбедности.

3.2.3. Процесни приступ

Стандард ISO 27001 усваја процесни приступ за успостављање, имплементацију, рад, праћење, преиспитивање, одржавање и побољшавање система менаџмента безбедношћу информација у организацији. Ради ефикасног функционисања, организација мора да управља многим активностима. Скуп активности које користе ресурсе и којима се управља да би се остварила трансформација улазних елемента у излазне, може се назвати процесом. Процесни приступ се, у том смислу, може оквалификовати као примена система процеса унутар организације, са идентификацијом и међусобним деловањем процеса и управљањем њима (Вујичић, Станковић, 2011).

Процесни приступ стандарда ISO 27001 заснива се на тзв. PDCA моделу: *Plan* (планирај) - *Do* (уради) - *Check* (провери) - *Act* (делуј, побољшај). Системи менаџмента безбедношћу информација структуирани су управо применом овог модела. На слици 2. приказан је PCDA концепт.

Слика 2. PCDA модел

Извор: ISO, 2013, прилагођено

У наведеном концепту који се базира на континуираном побољшавању, први корак представља план, други корак представља рад на спровођењу теста/испитивања, поређења или експеримента, по могућности у малој размери, у складу са оним што је одлучено у првом кораку. Трећи корак представља студију резултата (преистипитавање шта смо добро урадили, а шта нисмо). И, на крају, четврти корак представља акцију - усвајање или напуштање промене. Након ових корака, поново се пролази читав круг, можда под другачијим условима, са другим материјалима, људима или другачијим правилима (Атанасијевић, 2009). На Табели 2. описани су наведени кораци, а примењено на систем менаџмента безбедношћу информација.

Табела 2. PCDA модел у систему менаџмента безбедношћу информација (ISMS)

Планирати (успоставити ISMS)	Успостављање ISMS политике, циљева, процеса и процедура, које су битне за менаџмент ризиком и побољшање безбедности информација да би били постигнути резултати у складу са укупном политиком и циљевима организације.
Урадити (имплеметирати и примењивати ISMS)	Имплементација и примена ISMS политике, процеса, процедура и контрола.
Проверити (пратити и преиспитивати ISMS)	Оцењивање и мерење перформанси процеса у односу на политику, циљеве, искуство у пракси и израда извештаја који се односе на преиспитивање од стране руководства.
Деловати (одржавати и побољшавати ISMS)	Предузимање корективних и превентивних мера, заснованих на резултатима интерних провера ISMS и преиспитивањеима од стране руководства или другим информацијама ради постизања сталног побољшавања ISMS.

Извор: ISO, 2013, прилагођено

3.2.4. Сертификација

Организација може бити сертификована у складу са ISO 27001 од стране акредитованих регистара широм света. Сама ISO 27001 сертификација, као и остали ISO сертификати управљања системима, обично примењује три степена ревизије процеса:

1) „врх табеле“ - преглед постојеће и комплетне документације као што су организациона безбедносна политика, изјава применљивости и план поступка ризика;
2) детаљна, дубока ревизија која укључује тестирање постојања и ефективност информационих сигурносних контроли наведених у изјави применљивости и плану поступања по ризику, као и њихових помоћних докумената;
3) праћење поновне процене ревизије да би се потврдило да је претходна сертификациона организација остала у складу са стандардима (Атанасијевић, 2009).

Након што се сертификује, организација имплементира стандард у складу са његовим захтевима и процесним приступом.

ЗАКЉУЧАК

Да би уопште опстала на тржишту, организација мора да испуни више захтева, а један од њих је да усклади свој менаџмент систем са одговарајућим стандардима. Имплементација стандарда у пословање организације има позитиван утицај на свеукупно пословање организације. Један од врло важних стандарда који организације имплементирају у своје системе менаџмента јесте и стандард ISO 27001, који је управо обрађен у овом раду, а односи се на успостање система менаџмента безбедношћу информација, односно има за циљ да заштити организационе информације.

Информације у модерном пословном окружењу представљају кључне ресурсе организације, те је њихова заштита и безбедност од суштинске важности. Безбедност информација ставља се у први план, а њоме се мора позабавити највиши ниво менаџмента организација. Опстанак било које организације је у директној вези са њеном способношћу да сачува своје информационе вредности. Стога, концепт заштите информација долази на прво место, а обзиром да губљење информација, односно неадекватна заштита истих, може имати бројне негативне последице по пословање организације.

За заштиту и безбедност информација, као што се могло видети у раду, посебно је значајно увођење стандарда ISO 27001. Имплементација и примена овог стандарда доноси бројне предности организацијама, јер дефинише захтеве и приступе по којима се информације чувају. Да закључимо, основни циљеви који се постижу увођењем овог стандарда јесу: стална расположивост опреме и комуникација, заштита информација од неовлашћеног приступа, заштита података од губитка, заштита од цурења информација, осигурање континуитета пословања и пружање услуга за случај непредвиђеног догађаја.

На основу свега наведеног у раду, може се закључити да стандардом ISO 27001 свака организација представља својим корисницима и осталим заинтересованим странама да у току пословних подухвата послују на бази принципа сигурности и да је пословна политика усмерена на стална побољшања у систему менаџмента за безбедност информација. Употреба система заштите и безбедности информација, уверава клијенте и

пословне партнере организације да се она према информацијама односи одговорно и да се информације употребљавају и дистрибуирају на професионалан и безбедан начин. Организације које примењују захтеве овог стандарда, у тржишној су предности јер лакше стичу поверење својих клијената због предузимања свих мера која произилазе из стандарда. Уз то, стандардизација има свекупупан позитиван утицај на раст, развој и пословање организација.

ЛИТЕРАТУРА

Атанасијевић, С. (2009). *Безбедност информационих система.* Крагујевац.

Вујичић, С., Станковић, Р. (2011). ИСО менаџмент системи - садашњост и будућност. *Фестивал квалитета - 38. Национална конференција о квалитету* , А-125-130.

Вулетић, Д. (2011). Заштита критичних информационих структура. *Конференција о безбедности информација - зборник радова* .

Грубор, Г., Милосављевић, М. (2010). *Основе заштите информација, методолошко-технолошке основе.* Београд: Универзитет Сингидунум.

Драгишић, З., Радојевић, К. (2014). *Безбедносни менаџмент.* Београд: "Службени гласник".

Ђапић, М., Лукић, Љ. (2007). Стандарди серије ISO/IEC 27000 - Најбоља пословна пракса за сигурност информација. *"Фестивал квалитета". 34. Национална конференција о квалитету.* Асоцијација за квалитет и стандардизацију Србије.

Живковић, В., Крњајић, Д. (2009). Систем менаџмента безбедношћу информација - улога и значај сертификације и акредитације. *Сигурност информација, злоупотртебе информационих технологија- СИЗИТ09* .

Живковић, Н. (2012). *Интегрисани систем менаџмента.* Факултет организационих наука, Универзитет у Београду.

Закон о стандардизацији. „Службени гласник РС“, бр. 36/2009 и 46/2015.

ISO (2013). *ISO/IEC 27001 Information Security Management.* International Organization for Standardizationm.Доступно на: https://www.iso.org/standard/54534.html, приступљено: 10.08.2020.

ISO/IEC (2018). *ISO/IEC 27000: 2018 - Information technology - Security Techniques - Information security management systems - Overview and vocabulary.* Доступно на: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en, приступљено: 10.08.2020.

Kenning, M. (2001). Security management standard ISO 177799/BS 7799. *BT Technology Journal, Vol. 19, No. 3* , 132-136.

Латиновић, Т., Рољић, Л. (2014). *Управљање информацијама.* Бања Лука: Универзитет за пословни инжењеринг и менаџмент.

Протић, Д. (2013). Безбедност информација: стандарди или правила. *Војно дело, 65(1)* , 133-150.

Интернет извори:

https://www.kvalitet.org.rs/infrastruktura/standardi/iso-27001-i-iso-22301, приступљено: 10.08.2020.