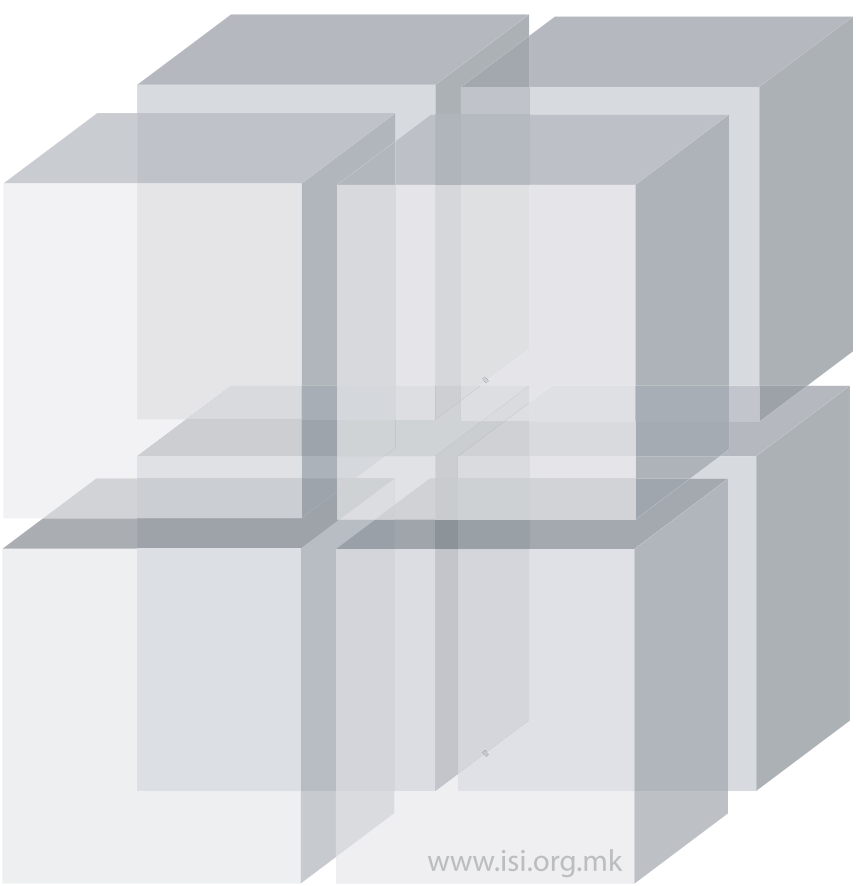
НАСОКИ ЗА ИНФОРМАЦИСКА СИГУРНОСТ

Проект „Иницијатива за информациска сигурност”

METAMORPHOSIS



METAMORPHOSIS

Насоки за информациска сигурност

Група автори

2007

Проект „Иницијатива за информациска сигурност“,
фондација „Метаморфозис“

Издавач
Фондација Метаморфозис
www.metamorphosis.org.mk

За издавачот
Бардил Јашари

Во изработката на документот учествуваа:
Сашо Мицков,
Љубомир Трајковски,
Неда Здравева,
Марјан Ристески,
Јован Петров и
Јорданка Петрушевска.

Поддржано од Фондација Институт отворено општество - Македонија
www.soros.org.mk

Графички дизајн и обработка:
Бригада дизајн
www.brigada.com.mk

Печати:
Про поинт - Скопје

СОДРЖИНА

ОСНОВНИ ДЕФИНИЦИИ И ПОИМИ

Информацијата е средство кое е од големо значење за функционирањето на секое општество, односно деловен процес и затоа треба да биде соодветно заштитена. Обезбедувањето на сигурноста на информацискиот систем ќе ја штити информацијата од различни типови закани и злоупотреби, за да се обезбеди деловен континуитет, да се минимизира штетата при работењето и да се максимизира продуктивноста и ефикасноста. Информацијата може да постои во многу форми. Таа може да биде печатена или напишана на хартија, да се чува во компјутер, да се пренесува преку пошта или со користење електронски средства или да се каже во разговор.

Информацискиот систем е систем со кој се прибираат, снабдуваат, чуваат, обработуваат, прикажуваат и испорачуваат информациите, со цел да бидат достапни и употребливи за секој што има право и потреба да ги користи. Информациските системи сè повеќе се соочуваат со закани и со изложеност на ризици од разни извори, вклучувајќи измами со помош на компјутер, шпионажа, хакерски упади или, пак, од таканаречените малициозни програмски кодови, односно вируси, кои се сè покомплексни и пософистицирани.

Информатичката и комуникациска технологија (**ИКТ**) се сите физички уреди и/или средства што се користат за автоматско прибирање, обработка, чување и презентација на информацијата. Во нашето секојдневие развојот на информацискиот систем ја користи информатичко-комуникациската технологија како средство за управување и манипулација на информацијата во сите фази на нејзиниот животен век.

Информатичката инфрастуктура ја опфаќа целата информатичко-комуникациска опрема во одреден ентитет - државен орган, организација, компанија или друг правен субјект во рамките на кои се создаваат, чуваат и обработуваат информациите.

Сопствениците на информацискиот систем се одговорни за планирање и за имплементација на организациските и технички мерки и контроли за постигнување на целите на сигурност, во согласност со важечките позитивни законски прописи и практики за обезбедување на сигурноста на информацијата во целиот нејзин животен век.

1. ВОВЕД

Воспоставувањето на сигурноста на информациските системи во сите сегменти на општественото и деловното опкружување е базична претпоставка за функционирање на информатичкото општество. Од друга страна, заложбата за создавање на услугите и содржините базирани на ИКТ (Информатички и комуникациски технологии) е еден од основните предуслови за зголемување на квалитетот на животот, но и за фаќање чекор со глобалните трендови.

Процесот за обезбедување сигурност на информацијата, врз база на нејзината точност, доверливост и достапност е основа за развој и за подобрување на севкупната бизнис-клима, унапредување на деловниот амбиент, заштита на приватноста на граѓаните, но и за просперитет на општеството. Важно е да се нагласи дека искуствата во земјите од развиениот свет недвосмислено потврдуваат дека вложувањето во високо технолошки решенија за информативна сигурност не се доволни за создавање поволен амбиент за непречено функционирање на информатичкото општество, ако тоа не е поткрепено со една поширока стратегија, препораки за користење, но и конкретни законски акти. Во тој контекст, зголемувањето на свесноста и потребата за сигурност и заштита на информацијата е од клучна важност во целиот систем на контроли и мерки како дел од услугите на информатичкото општество.

1.1. Информацијата како основен општествен фактор

Информацијата како општествен фактор и камен-темелник на постоењето и развојот на секое општество. Во време на транзиција кон економија базирана на знаења, основната компонента на знаењето, информацијата, база за обезбедување на конкурентната предност.

Република Македонија има определба да прерасне во информатичко општество базирано на знаење и ги прави сите напори таа определба да биде реализирана преку соодветни стратегиски документи и реализација на проекти. За таа цел е корисно сите

релевантни и засегнати субјекти (Владата, локалните самоуправи, приватниот сектор, јавниот сектор, граѓанскиот сектор, медиумите и секој индивидуален граѓанин) да имаат јасна визија за постигнување на таа зацртана определба.

Значењето на факторот информац ија има две димензии што треба да се земат предвид:

- **Позитивна димензија** – при што количеството и квалитетот на информациите директно влијаат врз добросостојбата и врз развојот на сите општествени вредности во државата. Протокот на информации има движечко и поттикнувачко значење.
- **Негативна димензија** – недостигот и „неквалитетот" на информацијата претставуваат директни закани за основните вредности врз кои се базира денешното општество и препреката за неговиот развој.

Животниот циклус на секоја информација ги содржи фазите на нејзиното креирање, организирано чување, обработка, користење и дистрибуција. Денес во секоја фаза на тој циклус нагласено битен фактор претставуваат ИКТ. Но, освен техничките, на интегритетот на информациските системи директно влијаат и човековиот фактор, организацискиот фактор, како и општествените и законските рамки во кои се одвива информацискиот животен циклус.

1.2. Информациска сигурност

Кај секој поединец постои потреба за основни предуслови и ресурси за опстојување. Задоволувањето на тие основни предуслови и ресурси ги задоволува само непосредните потреби. Како природна надградба следи потребата од расположивост на обезбедените потребни ресурси на подолг рок или на постојано. Таа надградба претставува нова потреба, која можеме да ја наречеме сигурност.

Непостоење сигурност, односно одземање на веќе обезбедени основни ресурси претставува криза. Видот на ресурсите со кои располага човештвото го одредува и името на епохата. Денес последниот ресурс во листата на основни човекови ресурси е ИНФОРМАЦИЈАТА како основа на ЗНАЕЊЕТО.

Необезбедените информации се причина за криза во помал или во поголем опсег. На денешно ниво, на користењето информации и информатички средства веројатноста за „информациски атак" е стварност. Последиците од денешните информациски напади се со голем степен на „штета" – поправлива или непоправлива.
Од тие причини, потребна е соодветна свесност за важноста и за потребата од информациска сигурност.

Современ феномен: Појава на информациска небезбедност

Основните општествени вредности секогаш биле цел на процесите на нивно обезбвреднување и злоупотреба. Иако процесите на обезвреднување и злоупотреба на информацијата биле секогаш присутни во сите фази на развојот на општеството, денес со развојот на ИКТ, тие се особено атрактивни.
Масовноста на современите информациски технологии во услови на несоодветно подготвени работни околини и отвореноста на комуникациските канали само ја потенцираат ранливоста на нашето општество. Со тоа се створени услови за потенцијална информциска „небезбедност”.
Бројот на идентификувани и регистрирани прекршоци на безбедносните критериуми е во експоненцијален пораст во сите држави во светот. Настанатите штети ги пречекоруваат прифатливите граници. Постои голем број на:

- прекршоци од најнизок ранг (пример, SPAM - праќање рекламни пораки без одобрение на примачот),
- прекршоци со понизок ранг (пример, вируси - кои го попречуваат нормалното работење на инфраструктурата)
- прекршоци со повисок ранг (пример, упад во информациски системи) и
- прекршоци од највисок ранг (пример, деструкција на битни општествени инфраструктурни системи: комуникациски системи, енергетски системи, транспортни системи).

Информациската небезбедност е присутна. Општеството во целина, но и секој граѓанин лично треба да се грижат за обезбедувањето услови за сигурност на информациите и ИКТ со кои се служат.

Во последната Студија за светските состојби со информациската сигурност (The Global State of Information security”- 2006) наведува:

- Важноста на информациската сигурност е препознатлива како фактор со многу висок приоритет за опстојувањето на организациите во приватниот и во јавниот сектор.
- Надзорот и управувањето со информациската сигурност е вообичаено доделена на член на управен одбор („CISO”- Chief Information Security Officer) и во многу примери интегрирана со т.н. „физичка сигурност”. Во тој случај се среќава и нов управувачки термин – „CSO”- Chief Security Officer .
- Финансиските вложувања за обезбедување на информациската сигурност во големите организации е поголем од 15 отсто од севкупниот ИТ буџет.
- Две третини од испитаниците (вкупно 8.000 директори на многу големи организации) сè уште немаат усвоено политики и стратегија за информациска сигурност.
- Повеќе од 90 отсто од организациите-учесници во студијата имале случаи со губење/крадење лаптоп на врвните директори во организациите.
- Повеќето од организациите ги фокусираат безбедносните мерки на ИТ ресурсите (информации, опрема, човечки ресурси).

Како заклучок:

- Свесноста за потребата од организиран и стратегиски пристап во обезбедувањето на информацискатa сигурност во организациите и во општеството е во подем.
- Појавата на информациски инциденти и вредноста на претрпените штети е во подем.
- Небезбедноста на информациите може да се надмине само доколку сите елементи, кои се составен дел на животниот век на информацијата, се погрижат за нејзината сигурност.

Во ерата во која најголемиот дел од протокот на информациите се одвива по електронски пат, логично се поставува прашањето за сигурноста на информациските системи (од технолошки, но и од општествен аспект). Сигурноста на информациските системи го обезбедува квалитетот, интегритетот, приватноста и доверливоста на податоците. Неопходно е зголемување на квалитетот на информациите поврзани со информацискатa сигурност, подигнувањето на јавната свест и системското поставување на неопходната општествена околина за сигурност и приватност на податоците. Овој документ претставува обид за подигнување на јавната свест, но и насока за општествената визија поврзана со информацискатa сигурност, како на ниво на институции, така и на ниво на фирми и граѓани.

Обезбедувањето на сигурноста на информациските системи е комплексен и пред сè континуиран процес, кој може да се разгледува на повеќе нивоа. Овој документ нема амбиции да ги покрие сите аспекти на управување со сигурноста, туку, пред сè, да служи како вовед и насока во формулирањето и во воспоставувањето адекватни стандарди и препораки, дефинирање на правата и одговорностите на учесниците во процесот на развојот и користењето на е-услугите. Овие насоки можат да послужат како вовед во изработката на идните политики и стратегиски документи поврзани со информацискатa сигурност и приватност, која потоа би се операционализирала и ефектуирала преку конкретни законски решенија и акти за правата, одговорностите и должностите на субјектите, односно корисниците на информациските системи.

Воспоставувањето на ваквата рамка и нејзиното имплементирање во сите нивоа не само што ќе биде основа за развој на информатичкото општество, туку и практично ја потврдува заложбата за хармонизација и за усогласување со современите европски и светски тековi.

Преку имплементацијата на мерките за сигурност на информацискиот систем, државните органи ќе може да развијат формални процедури и методи за справување со таканаречениот компјутерски криминал поткрепен со прецизни и јасно дефинирани истражни постапки и методи.

Заложбата за сигурни и ефикасни информациски системи опфаќа широк спектар активности кои е невозможно да се изведат без соодветна системска поставеност на информацискатa сигурност на национално ниво. Според тоа, од витално значење е Република Македонија да прифати и да промовира релевантни, меѓународни стандарди во поглед на сигурноста. Примената на овие стандарди ќе обезбеди зголемена заштита на информациите што се чуваат, односно се обработуваат во/преку информациските системи на еден систематски и ефикасен начин.

Тргнувајќи од основното начело дека:

„Сигурноста на информацискиот систем е обврска на секој учесник во процесот”

потребно е да се разработи методологија за соодветно алоцирање на правата, должностите и одговорностите во еден заокружен систем за управување со сигурноста. На пример, во процесот на дефинирање на законските рамки од клучна важност е одговорноста, пред сè, на државните органи како двигатели, односно носители на целиот процес за усогласување со законските прописи во ЕУ, кои потоа би се ефектуирале во сите сегменти и сфери од дејствувањето. Врз основа на ваквите начела и препораки, сите учесници-корисници на услугите на информатичкото општество се должни да се придржуваат кон највисоките стандарди на однесување и чесност во секоја комуникација и користење на информациите, како вистински и реален придонес во градењето на доверливоста, интегритетот, ефикасноста и квалитетот на процесите и услугите.

2. ЗАКОНСКА РАМКА ЗА ИНФОРМАЦИСКАТА СИГУРНОСТ

2.1. Анализа на постојната законска рамка

Низа закони во Република Македонија ги регулираат прашањата поврзани со информациите (лични податоци, класифицирани информации) и институциите што поседуваат информации и располагаат со нив, кои треба да се имаат предвид при определувањето на системот за обезбедување сигурност на информациските системи. Она што е карактеристично е дека ниту еден закон не оперира со терминот „информациска сигурност”, иако законите создаваат рамка, а соодветно определни надлежни државни органи обезбедуваат висок степен на заштита на тајноста на податоците.
Законодавството што постои во моментов, во определена мера ги задоволува стандардите на ЕУ, како и оние на НАТО, кои особено треба да се земат предвид во контекст на информацискатa безбедност при државните безбедносни системи.
Во ова поглавје прикажани се законските подрачја кои се клучни за воведување современ концепт на информациска сигурност, но и областите кои во поширок контекст го допораат прашањето на информациите - нивното собирање, чување, користење, а оттука и нивната безбедност.
Законот за класифицирани информации („Службен весник” на РМ 9/04) ја уредува класификацијата на информациите, условите, критериумите, мерките и активностите што се преземаат за заштита на информациите, правата и обврските на оние што ги создаваат и користат информациите, меѓународната размена и други прашања поврзани со класификацијата на информациите. Негова цел е да обезбеди законито користење на класифицирани информации и оневозможување секаков вид незаконски пристап до информациите.

Законот дава дефиниции на неколку поими кои се од основно значење за сигурноста на информациските системи. Во согласност со Законот (член 5):
- „информацијата” е сознание што може да биде пренесено во која било форма;
- „класифицирана информација” е информацијата што се заштитува од неовластен пристап или употреба и која се определува со степен на класификација;
- „безбедносен ризик” е можност за нарушување на безбедноста на класифицираната информација;

- „безбедност на класифицираната информација" се активности и мерки со кои се обезбудва заштита на класифицираните информации од неовластен пристап и употреба;

Информациите што се предмет на класификација особено се однесуваат на: јавната безбедност, одбраната, надворешните работи, безбедносните, разузнавачките и контраразузнавачките активности на органите на државната управа на РМ; системи, уреди, проекти и планови од важност за јавната безбедност, одбраната, надворешните работи; научни истражувања и технолошки, економски и финансиски работи од значење за Република Македонија. Класификацијата на информациите се врши според нивната содржина, при што постојат четири степени на класификација: (1) државна тајна, (2) строго доверливо, (3) доверливо и (4) интерно. Со законот се определува кој вид информации ќе се класифицираат соодветно на определените степени.
Законот определува критериуми, мерки и активности за заштита на класифицираните информации.

При утврдувањето на мерките за заштита на класифицираната информација се земаат предвид следниве критериуми:
- степенот на класификација
- обемот и формата на класифицираната информација
- проценката за заканата на безбедноста на класифицираната информација.

Со законот се определуваат низа мерки и активности за административна, физичка, информатичка и индустриска безбедност, како и безбедност на лицата.

Мерки и активности за информатичка сигурност, во согласност со член 28, се:
- сертификација на комуникациско-информациски системи и процеси;
- процена на можно нарушување на безбедноста на класифицираната информација со упад во информатичкиот систем и употреба и уништување на класифицираната информација обработувана и чувана во комуникациско-информациските системи
- утврдување методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицирани информации во електронска форма;
- заштита на информациите при процесирање и чување на класифицирани информации во комуникациско-информациските системи;
- продукција на крипто-клучеви и друг крипто-материјал;
- криптографска заштита на комуникациски, информациски и други електронски системи преку кои се подготвуваат, пренесуваат, обработуваат и архивираат класифицираните информации;
- определување зони и простории заштитени од компромитирачко електромагнетско зрачење и
- инсталирање уреди за чување на класифицираните информации.

Заштитата на личните податоци како основни слободи и права на граѓаните, а особено правата на приватност во врска со обработката на личните податоци, се остварува во согласност со **Законот за заштита на лични податоци** („Службен весник” на РМ бр. 7/05), кој ја обезбедува правната и институционалната рамка за заштита на податоците.

Во согласност со овој Закон (член 2, точка 1):

- „личен податок” е секоја информација што се однесува на индентификувано физичко лице или физичко лице што може да се идентификува, а лице што може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на единстен матичен број на граѓанинот или врз основа на едно или повеќе обележја, специфични за неговиот физички, ментален, економски, културен или социјален идентитет.
- „обработка на лични податоци” е секоја операција или збир на операции што се изведуваат врз лични податоци, на автоматски или на друг начин, како што се: собирање, евидентирање, организирање, чување, приспособување или промена, повлекување, консултирање, употреба, откривање преку пренесување, објавување или правење достапни на друг начин, изедначување, комбинирање, блокирање, бришење или уништување.
- „контролор на збирка лични податоци” е физичко или правно лице, државен орган или друго тело, кое самостојно или со други ги утврдува целите и начинот на обработката на личните податоци.

Обработката на личните податоци по правило се врши со претходно добиена согласност од субјектот на личните податоци. Забранета е обработката на посебни категории лични податоци, а тоа се податоци што го откриваат расното или етничкото потекло, политичкото , верското или друго уверување, членство во синдикална организација и податоци што се однесуваат на здравствената состојба или на сексуалниот живот. Посебен режим на заштита се предвидува за обработката на единствениот матичен број на граѓанинот.

Законот предвидува тајност и заштита на обработката на личните податоци. Секое лице што има пристап до збирка лични податоци во име на контролорот или обработувачот на збирката лични податоци, вклучувајќи го и самиот обработувач на збирката лични податоци, должен е да обезбеди тајност, заштита на лични податоци и да ги обработува во согласност со овластувањата и инструкциите добиени од контролорот, доколку не е утврдено поинаку со друг закон.
За да се обезбеди тајност и заштита на обработката на личните податоци на субјектот, контролорот мора да примени соодветни технички и организациски мерки што одговараат на опремата и на трошоците што се потребни за нивно спроведување, а се однесуваат на:

- оневозможување на случајно или незаконско уништување на податоците од збирките лични податоци;
- оневозможување на неовластено преправање, откривање или пристап при обработката на личните податоци од збирката лични податоци;
- оневозможување на незаконска обработка на личните податоци од збирките лични податоци, особено доколку вклучува пренос на податоци преку мрежа;
- оневозможување пристап на неовластени лица до опремата што се користи за обработка на збирката лични податоци;
- оневозможување неовластено читање, копирање, промена или отстранување медиум на кој е сместена збирката лични податоци;
- оневозможување неовластено читање, внесување, промена или бришење на податоците од збирката лични податоци;
- оневозможување пристап на корисниците на збирките лични податоци до податоци за кои немаат право да ги обработуваат;
- можноста дополнително да се провери кој пристапил до системот и кои податоци од збирката лични податоци ги читал, внел, променил или избришал, во кое време го направил тоа и од кој уред пристапил;
- оневозможување неовластен пристап до збирката лични податоци од друга локација преку комуникациски уреди;
- оневозможување читање, копирање, промена или бришење податоци при нивен пренос преку комуникациски уреди или при транспорт на медиумот на кој е сместена збирката лични податоци;
- можност да се провери преку комуникациски уреди од кои локации може да се пристапи до податоците;
- организирање на работата во согласност со посебните барања за заштита на збирката лични податоци и
- оневозможување други форми на незаконска обработка.

Овие мерки треба да обезбедат степен на заштита на личните податоци соодветно на ризикот при обработката и природата на податоците што се обработуваат. Примената на соодветни технички и организациски мерки ја пропишува директорот на Дирекцијата за заштита на личните податоци[1]. Контролорот и обработувачот на збирката лични податоци должни се да водат евиденција на преземените технички и организациски мерки. Законот во голема мера е усогласен со директива 95/46/ЕК на Европскиот парламент и на Советот на Европа од 24 октомври 1994 за заштита на личните податоци и слободното движење на податоците и конвенција бр.108/81 за заштита на физичките лица, која се однесува на автоматската обработка на личните податоци, Совет на Европа[2].

[1] Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци е донесен на 19 декември 2005 година http://www.dzlp.gov.mk

[2] г-ѓа Маријана Марушиќ, директор на Дирекцијата за заштита на личните податоци, презентација на втората меѓународна конференција е-Општество.Мк, 15.11.2006

Законот за слободен пристап до информации од јавен карактер („Службен весник” на РМ 13/06) ги пропишува условите, начинот и постапката за остварување на правото на слободен пристап до информациите од јавен карактер со кои располагаат имателите на информации[3]. Правото на пристап до информациите го опфаќа правото на лицето овластено да побара информација (сите физички и правни лица) и да добие информација од имателите на информации, како и обврска на имателите на информациите нив да ги направат достапни до јавноста.
Правото на пристап до информациите не ја исклучува потребата за заштита на информациите и грижата за нивната безбедност и не значи дека сите имаат право на присатп до сите инфоамции што ги поседуваат, со кои располагаат или што ги надгледуваат органите на јавната власт (државни или локални).

Имателите на информации ќе одбијат барање за пристап до информацијата, ако побараната информација е:

- класифицирана информација со соодветен степен на тајност;
- личен податок чие откривање би значело повреда на заштитата на личните податоци;
- информација за архивското работење, која е утврдена како доверлива;
- информација чие давање би значело повреда на доверливоста на даночната постапка;
- информација стекната или составена за истрага, кривична или прекршочна постапка, за спроведување управна и граѓанска постапка, а чие давање би имало штетни последици за текот на постапката;
- информација што се однесува на комерцијални и на други економски интереси, вклучувајќи ги и интересите на монетарната и фискална политика и чие давање ќе има штетни последици во остварувањето на функцијата;
- информација од документ што е во постапка на подготвување и сè уште е предмет на усогласување кај имателот на информации, чие откривање би предизвикало погрешно разбирање на содржината;
- информација за заштита на животната средина, која не е достапна до јавноста поради заштитата на здравјето на луѓето и животната средина и
- информација што ги загрозува правата од индустриска или од интелектуална сопственост (патент, модел, мостра, стоковен и услужен жиг, ознака на потеклото на производот).

Пристапот до овие информации може да се одобри со исклучок ако со објавувањето на таквата информација, последиците врз интересот што се заштитува се помали од јавниот интерес, кој би се постигнал со објавувањето на информацијата.
Законот за електронски комуникации („Службен весник” на РМ 13/05) предвидува обврска за операторите на јавни комуникациски мрежи и давателите на јавни комуникаци-

[3] органите на државната власт и други установи и институции утврдени со закон, органите на општините, на градот Скопје и на општините во градот Скопје, јавните установи и служби, јавните претпријатија, правни и физички лица што вршат јавни овластувања и дејност од јавен интерес, утврдени со закон

ски услуги, поединечно или заеднички, доколку е потребно да донесат соодветни технички и организациски мерки за да обезбедат заштита на нивните мрежи и/или услуги. Мерките мора да обезбедат ниво на безбедност и заштита соодветна на можни ризици, при чие утврдување е потребно да се имаат предвид техничката оправданост и применливост.

Доверливоста на комуникациите се однесува на а) содржината на комуникациите; б) податоците за сообраќајот и локацијата кои се однесуваат на комуникациите и в) неуспешните обиди за воспоставување конекција. Во согласност со Законот (член 111, став 2) забранети се сите форми на следење, прислушување, прекинување, снимање, чување, пренесување и пренасочување на комуникациите. Операторите на јавните комуникациски мрежи и давателите на јавни комуникациски услуги, нивните застапници, вработените, претставниците и другите лица под нивно раководство и контола се должни да ја штитат доверливоста на комуникациите и по престанувањето на активностите во текот на кои тие биле обврзани да ја штитат доверливоста. Снимањето на комуникациите е под посебен режим во законот. Тоа е дозволено заради обезбедување доказ на пазарните трансакции или за каква било друга деловна комуникација или во рамките на организациите што примаат итни повици заради нивна евиденција, идентификација и постапување.

Прислушувањето на комуникациите, како начин на пристап до информациите, е законски регулирано. **Законот за следење на комуникациите** („Службен весник" на РМ бр.121/06) ги уредува условите и постапката за следење на комуникациите, начинот на постапување, чување и користење на добиените информации и податоци со примената на овој закон и контролата на законитоста на следењето на комуникациите. Следењето на комуникациите се врши со наредба на надлежен суд, освен ако му се наменети или постои согласност на лицето или лицата што се вклучени во комуникацијата. Во согласност со законот за електронски комуникации, операторите, преку кои се врши законското прислушување на комуникациите, се должни да обезбедат трајна евиденција за законското прислушување на комуникациите и да ги заштитат овие податоци како тајна во согласност со законот. Сите податоци, списи и други материјали собрани преку следење на комуникациите се доставуваат до надлежниот суд во рокот определен со наредбата за следење на комуникациите и тие се чуваат под посебен режим од страна на судот.

Кривичното законодавство претрпе измени кои доведуваат до инкриминација на делата насочени кон загрозување на приватноста и на информатичката сигурност. Кривичниот закон на РМ („Службен весник" на РМ бр. 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06) во член 147 - Повредата на тајноста на писма или на други пратки предвидува парична казна или казна затвор до 6 месеци за лицето, кое без судска одлука или согласност на лицето на кое му се упатени, ќе отвори туѓо писмо, телеграма, некое друго затворено писмо или пратка или обезбедена електронска пошта или на друг начин ќе ја повреди нивната тајност или ќе задржи, прикрие, уништи или на друг ќе му предаде

туѓо писмо, телеграма, затворено писмо или пратка или обезбедена електронска пошта. Ако делото е сторено со намера за себе или за друг да се прибави корист или да се нанесе штета, делото ќе се казни со парична казна или казна затвор до 1 година. Ако делото е сторено од службено лице, казната е од три месеци до три години, односно од три месеци до пет години. Гонењето се презема по приватна тужба. Во случаите на злоупотреба на лични податоци (член 149), лицето кое, во спротивност на условите утврдени со закон, без согласност на граѓанинот, прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година.Оваа казна му се заканува и на лицето што ќе навлезе во компјутерски иинформатички систем на лични податоци, со намера да ги користи за себе или за друг, да оствари некаква корист или да му нанесе некаква штета на друг. Ако делото го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три години, а доколу го стори правно лице, ќе се казни со парична казна. Казнив е и обидот за извршување на ова дело. Во согласност со КЗ, (член 149-а) тој што неовластено спречува или ограничува друг во пристапот кон јавниот информатички систем, ќе се казни со парична казна или со затвор до една година. Ако делото го стори службено лице во вршење на службата или одговорно лице во јавен информатички систем, ќе се казни со парична казна или со затвор од три месеци до три години. Гонењето се презема по приватна тужба. Неовластеното прислушување и тонско снимање е санкционирано на начин, кој законот со член 151 предвидува парична казна или затвор до 1 година за лицето кое со употреба на посебни уреди, неовластено прислушува или тонски снима разговор или изјава што не му е наменета. Со оваа казна ќе се казни и тој што ќе му овозможи на неповикано лице да се запознае со разговор или со изјава која е прислушувана или тонски снимана, како и лицето што тонски ќе сними изјава што му е наменета, без знаење на оној што ја дава, со намера да ја злоупотреби или да ја пренесе врз трети лица или тој што таквата изјава непосредно ја пренесува врз трети лица. Ако делото го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три години. Гонењето за делото се презема по приватна тужба, освен во случаите кога е сторено од службено лице.

Во кривичните дела против имотот, КЗ ги нормира: оштетување и неовластено навлегување во компјутерски систем (член 251), правење и внесување компјутерски вируси (член 251-а) и компјутерска измама (член 251-б). Оштетувањето и неовластеното навлегување во компјутерскиот систем подразбира парична казна или казна затвор до три години за лицето што неовластено ќе избрише, измени, оштети, прикрие или на друг начин ќе направи неупотреблив компјутерски податок или програма или уред за одржување на информатичкиот систем или ќе го оневозможи или отежне користењето на компјутерскиот систем, податокот или програмата или компјутерската комуникација. Оваа казна е предвидена и за лицето што неовластено ќе навлезе во туѓ компјутер или систем, со намера искористување на неговите податоци или програми заради прибавување противправна имотна или друга корист за себе или за друг или предизвикување имотна или друга штета или заради пренесување на компјутерските податоци што не му се наменети и до кои неовластено дошол на неповикано лице. Притоа ако со извршу-

вањето на овие дела е прибавена поголема имотна корист или е предизвикана поголема штета, казната е затвор од шест месеци до пет години. Ако овие дела се сторени кон компјутерски систем, податоци или програми што се заштитени со посебни мерки на заштита или се користат во работењето на државните органи, јавните претпријатија или јавните установи или во меѓународни комуникации или како член на група создадена за вршење такви дела, казната е затвор од една до пет години, а кога со сотрување на делото е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со затвор од една до десет години. Лицето што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети или погодни за извршување на овие дела ќе се казни со парична казна или со затвор до една година. Обидот за делото е, исто така, казнив, а посебните направи, средства, компјутерските програми или податоците наменети за извршување на делото се одземаат.

Лицето што ќе направи или ќе преземе компјутерски вирус од друг, со намера за внесување во туѓ компјутер или компјутерска мрежа, ќе се казни со парична казна или со затвор до една година. Тој што ќе предизвика штета во туѓ компјутер, систем, податок или програма со употреба на компјутерски вирус ќе се казни со затвор од шест месеци до три години, а ако со делото е предизвикана поголема штета или делото е сторено во состав на група создадена за вршење такво дело, сторителот ќе се казни со затвор од една до пет години. Казнив е и обидот. Компјутерската измама е кривично дело од понов датум. Со член 251-б се определува дека лицето кое со намера за себе или за друг ќе прибави противправна имотна корист со внесување во компјутер или информатички систем невистинити податоци, со невнесување на вистинити податоци, со фалсификување на електронски потпис или на друг начин ќе предизвика невистинит резултат при електронската обработка и преносот на податоците, ќе се казни со парична казна или со затвор до три години. Ако сторителот прибавил поголема имотна корист, ќе се казни со затвор од три месеци до пет години, а ако сторителот прибавил значителна имотна корист, ќе се казни со затвор од една до десет години. Тој што ја сторил компјутерската измама само со намера да оштети друг ќе се казни со парична казна или со затвор до една година. Ако со делото е предизвикана поголема штета, сторителот ќе се казни со затвор од три месеци до три години. (6) Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети за извршување на делото, ќе се казни со парична казна или со затвор до една година. Казнив е и обидот, а посебните направи, средства, компјутерски програми или податоци наменети за извршување на делото ќе се одземат. Сигурноста на информациските системи се од посебна важност при обезбедувањето на електорнската трговија. Иако ова прашње во Република Македонија не е сè уште целосно законски уредено, одредбите што се поврзани со тоа се наоѓаат во Законот за облигациски односи и во Законот за податоци во електронски облик и електронски потпис.

Во согласност со **Законот за облигациски односи** („Службен весник" на РМ 18/01 и 4/02) примањето и испраќањето изјави на волјата со цел склучување договор е можно

и преку електронски пат (член 23, 23-а, 23-б и 23-в), како и составувањето исправа како форма на договорот (член 64). Притоа треба да се обезбеди сигурност за идентитетот на испраќачот и на содржината на информацијата.

Електронското работење, кое вклучува употреба на информатичка и телекомуникациска технологија и употреба на податоци во електронски облик и електронски потпис и во судски, управни постапки во платниот промет е уредено и регулирано со **Законот за податоци во електронски облик и електронски потпис** („Службен весник” на РМ бр. 34/01). Со овој закон се определува времето и местото на праќање и прием на електронската порака; начинот на зачувување на документи, записи и податоци на електронски начин; електронскиот потпис и неговата доказна форма, начинот на издавање на квалификувани сертификати, нивната форма и содржина, како и правата и обврските на издавачите на сертификати. Законот предвидува казни за несоодветно чување или употреба на податоците и средствата за електронско потпишување.

Специфични закони што уредуваат прашања на различни евиденции содржат одредби за заштита на податоците со кои располагаат.

На пример, еден од нив е **Законот за матична евиденција за осигурениците и корисниците на правата на пензиско и инвалидско осигурување** („Службен весник” на Република Македонија бр. 16/04). Со овој закон се уредува матичната евиденција за осигурениците и корисниците на правата од пензиско и инвалидско осигурување, која содржи податоци потребни за остварување на правата од пензиско и инвалидско осигурување. Во матичната евиденција се водат податоци за осигурениците, корисниците на правата од пензиското и инвалидското осигурување и обврзниците за плаќање придонес за пензиско и инвалидско осигурување. Во прибирањето, обработката, користењето, размената и во чувањето на податоците, според овој закон, се применуваат одредбите од законот што ја уредува заштитата на личните податоци, ако со овој закон поинаку не е определено. Матичната евиденција ја воспоставува и ја води Фондот за пензиско и инвалидско осигурување на Македонија. Таа се води така што податоците определени со овој закон, се доставуваат по електронски пат во пропишан електронски облик, а по исклучок врз основа на пропишани обрасци на пријави и се внесуваат во средствата за автоматска обработка на податоците од фондот. Документацијата од матичната евиденција се чува во електронски медиуми заради обезбедување репродукција на податоците во оригинален формат. Заштитата на податоците, фондот ја обезбедува преку преземање мерки против неовластен пристап или неовластена обработка, како и мерки со кои се спречува уништувањето, губењето, промената, злоупотребата и неовластената употреба на податоците. Техничките и организациски мерки за обезбедување на податоците од матичната евиденција, фондот ги определува со општ акт.
Кога станува збор за заштита на информаците и законодавството што го уредува ова прашање, предвид треба да се земе и **Уредбата за канцелариско и архивско работење**

(„Службен весник" на РМ, бр 58/1996 год). Со овој пропис се уредува начинот на работа и правилата на постапување со документарниот материјал и архивската граѓа во канцелариското и архивско работење на сите иматели во Република Македонија (државни органи, претпријатија и други правни лица).
Првиот дел од уредбата, кој се однесува на „канцелариското работење", ги регулира следниве прашања: прием, прегледување, распоредување и заведување на актите, нивно доставување за работа и административно-техничко обработување, разведување и класифицирање на актите, одлагање на решените акти во писарницата. Вториот дел од уредбата се однесува на „архивското работење" на имателите. Во него се регулираат следниве прашања: одбирање на архивската граѓа од документарниот материјал; евидентирање и категоризација на архивската граѓа; попишување и уништување на документарниот материјал; чување, заштита и обезбедување на материјалот и граѓата; предавање на архивската граѓа во Државниот архив.
Уредбата дефинира обврска одбраната архивска граѓа да се чува, обезбедува и да се заштитува од секаков вид отуѓување, оштетување и уништување, меѓутоа не предвидува посебни правила за начинот на кој ќе се спроведува оваа обврска.

2.2. Меѓународни иницијативи

Директивата 46/95/ ЕЗ позната и како Директива на ЕУ за заштита на податоците (European) поставува барање до земјите-членки да усвојат национална регулатива со која ќе се стандардизира заштитата на приватноста на податоците на граѓаните низ цела Европска Унија. Законите за задржување на податоците (EU) бараат од лицата што обезбедуваат јавни комуникациски услуги (интернет и телефонија) да чуваат податоци за секоја испратена електронска порака и остварен телефонски повик во периодот од 6 месеци до 2 години.

Со резолуцијата на Советот на ЕУ 2002/С 43/02 од 28/01/2002 се дефинирани специфични активности во рамките на мрежната и информациската сигурност за земјите-членки, во кои спаѓаат:

- Промоција на стандардот ISO 15408 (Common Criteria), со цел да се усогласат различните подрачја и имплементации на сигурносните контроли;
- Примена на интероперабилни сигурносни решенија втемелени на препознатливи и потврдени норми и технологии (на пример, користење дигитални сертификати и потписи) во е-услугите имплементирани во земјите-членки на ЕУ;
- Соработка меѓу институциите во поглед на компјутерскиот криминал, односно воспоставување унифициран тим за реакција и справување со сигурносните ризици и напади преку формирање на таканаречениот инцидент менаџмент тим - (CERT – Computer Emergency Response Team).

Дополнително, преку акцискиот план за е-Европа (**i2010** - A European Information Society for growth and employment) се предлага формирање и функционирање на Cyber security

task force (CSTF), преку кој ќе се реализира висок степен на сигурност преку размена на класифицирани информации по строго утврдени правила и норми. Дополнително, во сите свои законски акти и програми за развој на е-услугите може да се препознае јасната и недвосмислена заложба на ЕУ и на нејзините органи за усогласување на законските норми за системско решавање на прашањата и проблемите во сите сфери од дејствувањето во поглед на информативната сигурност. Во таа насока, во согласност со уредбата на Европскиот парламент и Советот на Европа воспоставена е Европска агенција за мрежна и информатичка сигурност наречена: (*European Network and Information Security Agency – ENISA*, Regulation of the European Parliament and the Council of 10 March 2004 (OJ L 77, 13 March 2004). Оваа агенција треба да ги координира, усогласи и да ги решава проблемите на ниво на владините органи, државните институции, но и да работи на една поширока основа во граѓанскиот и невладин сектор со цел да се обезбедат сигурни и квалитетни е-сервиси и услуги. *ENISA* (*www.enisa.europa.eu*) е замислена како централно место за координација на сите сигурносни активности во рамките на Европската Унија.

„Покрај овие европски - повеќе или помалку признаени и потврдени стандарди и иницијативи - треба да се напоменат и неколку законски акти и правилници што се донесени во САД, од кои како поважни може да ги наведеме:

- Computer Security Act of 1987 издаден од страна на National Institute of Standards and Technology (NIST) и се однесува, пред сè, на стандардите и на препораките што треба да ги исполнат компјутерските системи во државните органи. Посебно е интересен фактот што во овој текст како задолжителна активност се наведува потребата од постојана едукација и надградба на сите учесници и корисници на информациските системи што располагаат со чувствителни информации;
- GISRA – Government Information Security Reform Act of 2000;
- USA Patriot Act of 2001 со посебен акцент врз правилата и методите за следење на електронските комуникации и откривањето и компјутерскиот криминал.
- FISMA - „Federal Information Security Management Act” of 2002, USA.

Како поставен стандард треба да се имаат предвид и некои компаративни решенија. Законот за преносливост и одговорност за здравствено осигурување на САД (Health) поставува барање пред организациите што обезбедуваат здравствена заштита, организациите што обезбедуваат здравствено осигурување и работодавачите да обезбедуваат заштита и приватност на податоците за здравствената сотојба на корисниците на услуги, осигурениците, односно вработените.
Законот Грам-Лич-Блајлеј од 1999 на САД (Gramm-Leach-liley), познат и како Закон за модернизација на финансиските услуги, ги штити приватноста и безбедноста на приватните финансиски информации што ги собираат, чуваат и процесираат финансиските институции.
Законот Сарбанес–Оксли од 2002 (Sarbanes-Oxley), оддел 404, од компаниите што излегуваат на јавниот пазар на капитал бара да ја проценат ефективноста на нивната внатреш-

на контрола на финансиското известување во годишните извештаи, кои ги поднесуваат на крајот од секоја фискална година. Главните офицери за информации (Chief Information Officers) се одговорни за безбедноста, точноста и за веродостојноста на системите што управуваат и известуваат за финасиските податоци. Законот, исто така, наложува овие компании да бидат подложни на надворешна ревизија, која мора да провери, односно да потврди и да извести за валидноста на дадените извештаи од страна на компаниите.
Стандардот за безбедност на податоците на индустријата на платежните картички (Payment) утврдува низа значајни барања за унапредување на безбедноста на информациите на платните сметки. Тој е развиен од страна на водечките компании во индустријата на платежни картички вклучително American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International, како поддршка на процесот на усвојување на конзистентни мерки за безбедност на податоците на глобално ниво. Овој стандард опфаќа постапки за управување со безбедноста, политики, постапки, архитектура на мрежата, дизајн на софтвер и други критични заштитни мерки.

2.3. Стратегиски насоки

Каде можеме да ја лоцириме моментната состојба на Р. Македонија во однос на прашањата за информативната сигурност и кои се чекорите што треба да се преземат во најблиска иднина?

Пред сè, потребно е јасно и недвосмислено да се потврди заложбата на сите чинители во процесот: државни органи, компании, банки, финансиски институции, граѓански и невладини организации за имплементација на сигурен информациски систем реализиран преку воспоставување стандарди, правила, препораки, но и конкретни законски решенија кои ќе ја регулираат оваа област.
Оваа заложба потоа треба да се ефектуира и да се реализира преку конкретни активности и проекти, кои може да се разгледуваат на неколку нивоа:

- Унапредување на законската рамка со која се уредуваат постапките, мерките и контролата при воспоставувањето на сигурен информациски систем на сите нивоа;
- Хармонизација на практиките на национално ниво со најдобрите практики на ЕУ и на НАТО во поглед на информациската сигурност;
- Прифаќање на ISO 17799, односно ISO 27001 како национален стандард за сигурност на информациските системи;
- Изработка на национални и локални политики и стратегии за информациска сигурност;
- Имплементација на сигурносни контроли преку конкретни решенија произлезени од законските норми, односно националната програма;
- Формирање и промоција на национален CERT - Computer Emergency Response Team;

- Континуирана едукација и подигање на свеста и знаењето на корисниците на сите нивоа во поглед на информативната сигурност.

Стратегискиот пристап потоа ќе обезбеди да произлезат низа нови закони или дополнување на веќе постоечките акти и правилници, кои се во интерес на имплементацијата на сигурни информативни системи како основен предуслов за развој на е-услугите и сервисите, односно фаќање приклучок кон современиот свет, односно европската интеграција.

Националната стратегија за развој на информатичкото општество во Република Македонија во состав на својот акциски план ги содржи следниве проекти:

- ПР3.27 ИСО 17799
- ПР3.38 Национална политика за ИКТ безбедност
- П3.39 Безбедносна сертификација
- П3.40 Национално тело за ИКТ безбедност
- ПГ6.02 е-Сигурност

Воедно, националната стратегија за електронски комуникации, која моментно се наоѓа во собраниска процедура, има посебно поглавје за информациската сигурност.
Информациската сигурност е комплексно мултидисциплинарно подрачје, кое не може системски да биде уредено со еден закон. На Република Македонија на овој план и претстои системска разработка на законодавството, која ќе почне со идентификација на сите закони што уредуваат прашања на прибавување, користење и чување информации, нивна внатрешна хармонизација и хармонизација со законодавството на ЕУ и со стандардите на НАТО, како и развој на реални планови и мерки за соодветна имплементација на законодавството. Ова законодавство треба да биде само дел од целокупната национална стратегија за информациска сигурност, која треба да биде донесена во Република Македонија со учество на сите заинтересирани страни.
Развојот на стандардите и мерките за информациска сигурност го условува и користењето на информатичката технологија и развојот на информациската инфраструктура во државата. Со овие стандарди и мерки треба да се изедначи начинот на постапување со информациите, со оглед на нивната специфика кај различните органи и лица што прибавуваат, користат или управуваат со информации.
Зајакнувањето на сигурноста во овој момент на развој и барање директни странски инвестиции е особено важна во бизнис- секторот, оттука контролата на прибавувањето, чувањето и управувањето со информациите се јавува како иманентна потреба.
Детална анализа на законодавството и негова хоризонтална и вертикална хармонизација е еден од чекорите што треба да бидат преземени за обезбедување информациска сигурност.

3. СТАНДАРДИ

3.1. Систем за управување со информацискатa сигурност

Постигнувањето на информацискатa сигурност е континуиран процес, кој претставува комплексен систем од методологии, активности и мерки. Притоа, функционалниот и сигурен информациски систем во најширока смисла на зборот се темели на исполнувањето на следниве начела:

- **Доверливост** (анг. Confediality) - информацијата не смее да биде достапна или да биде откриена на неовластени лица;
- **Интегритет** (анг. Integrity) - информацијата не смее неовластено или непредвидено да се менува;
- **Достапност** (анг. Availability) - информацијата е достапна во моментот кога има потреба за тоа;
- **Неодречност** (анг. Non-Repudiation) - неможност за одрекување на активностите поврзани со користење и пристап на информациите;
- **Докажливост** (анг. Accountability) - активностите поврзани со манипулација и пристап до информацијата може да бидат еднозначно забележани и евидентирани;
- **Автентикација** (анг. Authentication) - идентитетот на субјекот и неговите права на пристап до информацијата може еднозначно да се утврди/идентификува и контролира.
- **Надежност** (анг. Reailability) - обезбедува очекувано и предвидливо однесување, односно состојба на информацискиот систем.

Нарушувањето на некои од овие начела, всушност, значи нарушување на сигурноста на информацискиот систем. Во основа може да се заклучи дека се можни следниве закани и потенцијални нарушувања на нормалното функционирање, кое може да доведе до:

Губење на интегритетот: Интегритетот, всушност, означува потреба информацијата и соодветните информатичко-комуникациски средства да бидат заштитетни од неовластени и несоодветни промени. Ваквите неконтролирани промени во содржината на информацијата значи нарушување на нејзината точност/коректност, односно компромитирање на нејзината валидност и применливост. Нарушениот интегритет на информацијата доведува до погрешно интерпретирање и донесување погрешни заклучоци.

Губење на достапноста: Практично, ова означува нарушување на нормалното – очекувано оперативно функционирање на информацискиот систем. Со други зборови, информацијата не е достапна во моментот кога е навистина потребна.

Губење на доверливоста: Неовластено, неавторизирано откривање и пристап до информациите од страна на субјекти/процеси кои немаат дозвола за тоа.

Процесот на информативната сигурност треба да биде дизајниран на начин што ќе овозможи, пред сè, да се идентификуваат, мерат, контролираат и да се следат ризиците поврзани со доверливоста, интегритетот и расположивоста на информациите на една континуирана основа. Ваквиот пристап промовиран од ISO 17799 и ISO 27001 е познат како PDCA (Plan – Do – Check – Act) модел, кој се состои од следниве целини (субпроцеси):

1. Планирање на процесот, кој опфаќа:

- Процена на ризикот - континуиран процес на идентификација на слабостите и заканите кон информативните системи. Процесот треба да ја идентификува можноста и фреквенцијата на појавувањето на заканите за да се утврди евентуалната штета, која би настанала доколку тие се случат;
- Изработка на политика за сигурност на информациските системи - секој сопственик на информацискиот систем е должен да донесе политика за сигурност на информацискиот систем, која ќе претставува стратегија (план) на менаџментот за управување со идентификуваните ризици (од претходниот чекор). Оваа политика треба да биде во согласност со програмата за информатичка сигурност на Р. Македонија, позитивните законски прописи, како и соодветните светски стандарди од оваа област (како што е ISO 27001/BS7799) и да биде практична потврда на посакуваното ниво на адекватна сигурност на информацискиот систем, во согласност со извршената анализа на ризиците и заканите;

2. Имплементација на сигурносни контроли - секој сопственик на информацискиот систем е должен да воспостави административни, физички и технички контроли со кои ќе се изврши заштита на сигурноста на информациите и системите на повеќе нивоа;

3. Тестирање и проверка на сигурноста - секој сопственик на информацискиот систем е должен да воспостави процес на професионално, независно и објективно тестирање и проверка на ефикасноста и адекватноста на имплементираните контроли содржани во политиката за информативната сигурност;

4. Надградба и корекција - секој сопственик на информацискиот систем е должен да воспостави процес на континуирано прибирање и анализа на информации од аспект на нови закани и слабости, актуелни напади кон информацискиот систем комбинирани со ефикасноста на постојните сигурносни контроли.

Управувањето со сигурноста е комплексен и континуиран процес, кој ги опфаќа: луѓето (субјекти), процесите, организациската поставеност и користена технологија и следствено тој треба да биде базиран на прецизно и јасно планирање, кое може да биде:

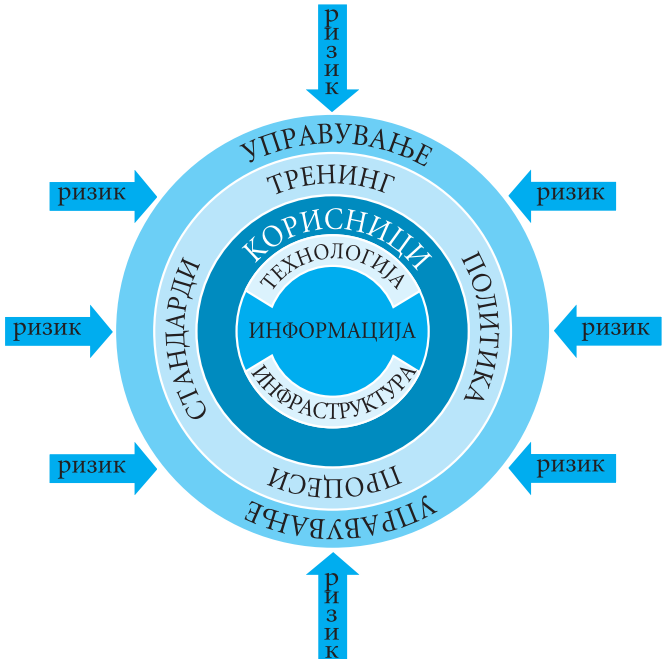
- Стратегиско, кое опфаќа прашања поврзани со посакуваното ниво на сигурност, целите и потребата за сертификација, односно акредитација;
- Тактичко или среднорочно, кое опфаќа дизајн и имплементација на планираните сигурносни контроли и мерки;
- Оперативно или краткорочно, кое опфаќа секојдневни активности и мерки за контрола и мониторинг на сигурноста (анг. day-to-day activity).

Сигурноста на информацискиот систем може да се обезбеди преку повеќе нивоа на контроли: физички, технички и административни. Овие три категории може дополнително да бидат поделени на контроли за спречување, за откривање или, пак, контроли што се користат за минимизирање, односно коригирање на евентуалните штети настанати како резулатат на нарушувањето на сигурносните начела.

- **Физички контроли** кои служат за обезбедување адекватна физичка сигурност во информативниот систем. Како примери на физички контроли се: употребата на брави, чуварска служба, бедеми, аларми и слични мерки за контрола на пристапот до ресурсите. Овие мерки имаат за цел да спречат можни закани од типот на шпионажа и саботажа, отуѓување и уништување или оштетување од несреќен случај или природна катастрофа (поплава, земјотрес...).

- **Технички или логички контроли** кои се вградени во информатичката опрема, апликативниот софтвер, комуникациската опрема и придружните уреди (како на пример: антивирусна заштита, енкрипција/шифрирање на преносот, автентикација, пристапни листи, употреба на огнени ѕидови - firewall и слично).

- **Административните контроли** вклучуваат воспоставување политики, стандарди, упатства.



Вистинското справување со овие прашања може да се реализира само преку координирани и усогласени системски решенија и мерки како составен дел од заокружен процес, односно како систем за управување со информативната сигурност (анг. ISMS – Information Security Management System). Процесот не е и не треба да биде само сет од технички контроли и мерки, туку, пред сè, тоа е еден заокружен и целосен систем на организациско-административни функционални решенија. Во таа насока може да се напомене BS 7799 (ISO 17799) како светски признат и познат модел и препораки за ефикасна имплементација на сигурносните мерки и контроли. Според овој стандард, секој систем за управување со информативната сигурност треба да ги содржи следниве 10 базични домени/елементи, како што следува:

- **Политика за сигурност** (анг. Security policy) - претставува темел на градењето на процесот на информациската сигурност. Таа треба да претставува работна рамка за изработка на дополнителни документи - процедури, стандарди и упатства, преку кој ќе се разработат и операционализираат заложбите за заштита на информацијата и соодветните контроли.

- **Организација и алокација на ресурси** (анг. Organization of assets and resources) - целта на овој домен е да ги дефинира и да постави системска и организациска поставеност и главни и специфични одговорности на субјектите од аспект на сигурноста на информацискиот систем.

- **Класификација и контрола на пристап** (анг. Asset classification and control) - информацијата мора да биде класифицирана според нејзината важност, валидност и вредност за функционирањето на системот. Класификацијата на информациите е основа за имплементација на сигурносните контроли и степенот на заштита што треба да се оствари.

- **Сигурност на субјекти** (анг. Personnel security) - го покрива аспектот на злоупотреба и нарушување на сигурноста предизвикана од намерно или случајно прекршување на правилата и мерките за сигурност. Секој учесник во процесот потребно е да биде свесен за своите одговорности и задачи преку прифаќање соодветен - кодекс за сигурност и доверливост. Како клучен фактор за успех во целиот процес е и постојаната едукација, односно развојот на програми и кампањи за подигање на свесноста и потребата од зголемување на нивото на сигурноста на информацискиот систем.

- **Физичка сигурност** (анг. Physical and environmental security) - многу безбедносни ризици можат да се избегнат ако се контролира физичкиот пристап до „високоризичните” ресурси во информацискиот систем. Физичките контроли вклучуваат низа превентивни мерки и мерки за детекција, како што се: чуварска служба, обезбедување рестриктивни и заштитени области за ресурсите од информацискиот систем со контролиран влез, обезбедување соодветни метални сефови за компјутерски и комуникациски уреди, поставување сензори и системи за набљудување и откривање, противпожарни системи и слично.

- **Комуникација и ракување со системите** (анг. Communication and operation management) - оперативна покриеност со процедури за ракување и обработка на информациите, реализација на организациска структура за поделба на активностите во системот - соодветна сегрегација на должности, справувње и реакција на инциденти при нарушување на сигурноста (анг. incident management).

- **Контрола на пристап** (анг. Access control) - секој информациски систем мора да го утврди начинот на кој се управува безбедноста при користењето на информациите и податоците од компјутерскиот систем; да направи јасна поделба на должностите и задачите (кому и што треба да му се дозволи) и одговорноста за интегритет и доверливост на податоците. Логичкиот пристап се дефинира преку имињата на корисниците и лозинките. Секој корисник на информациски систем мора да користи единствен идентификатор (корисничко име и лозинка) за најава (login) и за користење на информацискиот систем, кој се нарекува кориснички профил (user account).

- **Одржување и развој на системите** (анг. System development and maintenance) – обезбедува механизми и препораки за планирање и стратегија за развој и ракување/управување со системите. Потребно е соодветно да се документираат сите фази и аспекти од животниот век на експлоатацијата на информацијата (анг. Information lyfe cycle).

- **Континуитет во работењето** (анг. Business continuity management) - процесот на управување на континуитетот на работата треба да се спроведе со цел да се намалат ризиците за нарушување на функциите на информацискиот систем предизвикан од катастрофа, техничка неисправност и безбедносни напади и инциденти (кои можат да бидат резултат на природни катастрофи, несреќни случаи, дефекти на опремата, намерни постапки, саботажи итн.) на прифатливо ниво преку комбинација на превентивни и корективни контроли. Планот за континуитет на работата треба да се спроведе како збир на разработени процедури и постапки составени и одржани во готовност за користење во случај на итност или катастрофа. Планот за санирање катастрофи (анг. Disaster Recovery Plan) треба да се спроведе за насочување на процесот за санација/корекција на критичната информатичка и комникациска инфраструктура, во случај на прекин на постојаната услуга што настанува од непланирана и неочекувана катастрофа или инцидент.

- **Усогласеност со законските одредби** (анг. Compliance) - обезбедува постоење механизам (системски траги) за следење на сигурносните инциденти, мониторинг и имплементација на сигурносните барања и препораки пропишани од страна на соодветни и релевантни законски акти и стандарди.

3.2. Класификација на информации

Точната и навремена информација е од критична важност за ефикасноста на современото деловно работење, но и пошироко за функционирање на сите општествени процеси и активности. Сама по себе, информацијата може да се појави и да егзистира во различни форми и медиуми (пишани, говорни, електронски) со што значително се зголемува и нејзината изложеност на најразлични закани - намерни или случајни. Од исклучителна важност е да се идентификуваат слабостите на информативните средства и потенцијалните закани по нивниот интегритет, доверливост и достапност базирано, пред сè, на крајната чувствителност на информациите, која сама по себе е сложен и динамичен процес.
Информацијата мора да биде класифицирана според нејзината важност, валидност и вредност за функционирањето на информацискиот систем. Првиот и основен чекор во остварувањето на сигурноста на информацијата е нејзиното класифицирање, односно одредување на нејзината важност и сензитивност, односно влијанието врз нивото на сигурноста на целиот систем. Класификацијата на информацијата е вовед во спроведувањето на планот за успешна анализа и справување со потенцијалните ризици и опасности, кои можат да ја нарушат доверливоста и интегритетот. Таа е потребно да биде изведена преку точно одредени правила и мерки пропишани и усвоени од страна на сопственикот на информацискиот систем, во согласност со позитивните законски прописи и акти. За таа цел треба да се идентификуваат сите критични компоненти на системот, односно да се препознаат неговите граници, да се утврди чувствителноста и важноста на информатичката опрема - хардверот и софтверот, информациите што се чуваат, процесираат и транспортираат.

Класификацијата на системот претставува раслојување на информацискиот систем според чувствителноста на информацијата. Доколку не постои вреднување на чувствителноста на средствата и информациите, тогаш ќе се смета дека сите средства и информации се од највисок ранг на чувствителност и за сите нив треба да се применат соодветни сигурносни контроли.

Спроведувањето на класификацијата на информацијата е одговорност и должност на нејзиниот сопственик, односно сопственикот на информацискиот систем, но таа треба да биде направена во согласност со позитивните законски прописи и соодветните стандарди. На пример, во согласност со препораките на релевантните стандарди за сигурност на информациските системи во делот на државните органи постои следнава градација на информациите: некласифицирана, чувствителна, доверлива, тајна и врвна тајна. Во согласност со ваквите препораки потребно е да се изработат правилници за имплементација на класификацијата, која ќе ги опфати сите фази од нејзиниот животен век, од моментот на креирање, експлоатација, користење, архивирање, па сè до нејзиното бришење, односно целосно уништување. При разработката на методологијата за класификација, предвид треба да се земе и природата на информацијата, односно нејзината намена и местото на настанување (државен орган, банка, индустрија...). Како посебен облик на класификација на информацијата е, на пример, употребата на личните податоци за која постои законска регулатива во државава и според која посебно се пропишува начинот за нивното чување, дистрибуција или јавно презентирање. Меѓутоа, овој законски акт треба да се надополни и да се усогласи со една поширока работна рамка или методологија во која ќе бидат опфатени сите видови информации и нивна класификација (на пример, јавна информација, доверлива информација, тајна и врвна тајна).

При разработката на политиката и на методологијата за класификација и ракување со информациите како минимум треба да се земат предвид следниве моменти.

- Секој информациски систем мора да има прецизно дефинирани критериуми за класифицирање на информациите базирани на нивната вредност, критичност и важност за функционирањето на процесите;
- Информацискиот систем мора да имплементира заштитни механизми за информациите по обем и по големина соодветна на нивната важност;
- Процедурите и упатствата за манипулирање со податоците, односно информациите базирани на нивната важност треба да бидат јасни и прецизни и со нив да се запознаат сите учесници во процесот;
- За информациите што се предмет на законска регулатива, во смисла на нивно чување и манипулирање, сопственикот на информацискиот систем мора да ги следи одредбите од соодветните закони;
- Информацијата правилно ќе се заштити само доколку се специфицира нејзината важност, но и сопственоста, односно само доколку се направи јасна поделба на должностите во смисла кој е нарачател-сопственик на информацијата, кој е системски имплементатор на контролите, а кој е краен корисник на информацијата;

- Информациите треба да имаат механизам за означување („лабелирање”) на нивната важност со што би можело правилно да се третираат во согласност со процедурите и упатствата;
- Под заштитни механизми се подразбираат сите технички, административни и физички контроли и мерки, кои обезбедуваат интегритет, доверливост и достапност на информацијата, а се однесуваат на начинот на чување, транспорт и користење;
- Информацијата може да се декласифицира, односно да ја промени својата критичност и важност, при што треба да постои точно утврдена постапка под кои услови и кога престанува да важи соодветната класификација;
- Информациите класифицирани како врвна тајна со исклучителна важност за целиот процес мора да се третираат со највисок степен на заштита и пристапот до нив мора да биде строго дефиниран и контролиран;

3.3. Управување со ризици

Процената на ризикот кон сигурноста на информацискиот систем е чекор на идентификација на ризиците кон доверливоста, интегритетот и расположивоста на информациските системи. Процесот на процена на ризик е неопходен чекор за формирање стратегија и политика за сигурност на информациските системи. Почетната процена на ризик може да бара значителен еднократен напор, меѓутоа во натамошниот период таа треба да се одвива во континуитет.

Идентификацијата на заканите и слабостите (анг. risk assessment) е најзначајниот и базичен чекор кон имплементацијата на сигурен информациски систем. Процесот ја идентификува можноста и фреквенцијата на појавување на заканите и слабостите на информативните средства, со цел да се утврди ризикот од евентуалната штета која би настанала доколку тие се случат. Овие сознанија се основа за изградба на систем од контроли и мерки за минимизирање на ризиците, односно нивно управување и контролирање на разумно и прифатливо ниво (анг. risk management).

Управувањето и анализата на ризици е од исклучителна важност за одредување на таканаречената посакувано ниво на сигурност, односно мерка за прифатливост и адекватност на ризиците и контролите.

Причините за настанување на одреден разик може да бидат најразлични и тие може да се разгледуваат од повеќе аспекти и според повеќе критериуми. Во продолжение следат најчестите ризици за информативните средства групирани според нивната природа на настанување (анг. *risk factor*):

- **Ненамерните** закани опфаќаат инциденти од неадекватни интерни системи на контрола и неадекватни процедури во работењето, неадекватни контроли на пристап и недостиг од физичка сигурност или од природни катастрофи.
- **Намерните** закани обично изведени од страна на корисниците мотивирани од неетички или материјални причини (платен од конкуренција, поранешно вработен, незадоволен корисник), кој може да ги искористи слабостите на информацискиот систем.

Базирано на овие ризици потребно е прво да се согледа нивното влијание врз квалитетот и точноста на самиот процес, а потоа во согласност на тоа потребно е да се изработи стратегија/план за управување, односно контрола на ризикот, кој може да опфати:

- елиминација на ризикот
- минимизирање на ризикот
- трансфер на ризикот
- прифаќање на ризикот

3.4. Стандарди и препораки

Меѓународни ИСО стандарди

Како одговор на првите информациски инциденти и напади, првенствено во сферата на информациските системи и комуникациски мрежи, се појавуваат упатства - добри практики за обезбедување заштита на информациите и информациско-комуникациските средства. Согледувајќи ја потребата за поголема ефикасност на информацискаата сигурност на глобално ниво почнува процесот на доброволна регулација, т.е. појава на меѓународни стандарди (пример ИСО).

Постојната збирка стандарди главно се дели во две категории :

- Стандарди за информациска сигурност на информациско-комуникациските ресурси (т.н. технички стандарди)
  - ПРИМЕР : ИСО 15408 Information technology – Security techniques – Evaluation criteria for IT security
- Стандарди за обезбедување управувачки процеси за подобра информациска сигурност (т.н. менаџмент стандарди)
  - ПРИМЕР :
    - ИСО 17799 Information Security Management System- Guidelines
    - ИСО 27001 Information Security Management System- Specifications

Тргнувајќи од основниот принцип на доброволно придржување и примена на одредени стандари, се доаѓа до состојба ефектите на нивната примена да бидат далеку под очекувањата.

Во функција на подобрување на таквата состојба се појавува практика заинтересираните субјекти да бараат одредени организации и фирми да се придржуваат до одредени стандарди како предуслов за нивен ангажман.

Дури и во некои општествено битни индустриски сегменти (финансии, здравство) се појавуваат „обврзувачки", т.е. „елиминирачки" барања за придржување и примена на одредени стандарди(во финансискиот сектор – Басел 2 , во здравствениот сектор на САД - ХИИПА).

Меѓународни конвенции и декларации

Информациската небезбедност е идентификувана и е препознаена како заедничка опасност за сите. Со цел да се обезбеди заеднички одговор, релевантните меѓународни институции, како Обединетите нации, ОЕЦД, Европската Унија, имаат донесено соодветни резолуции и препораки за своите земји-членки како да се пристапи кон воведување потребни мерки за обезбедување на информациите, т.е. за спречување масовна појава на информациската небезбедност.

Постоењето на тие резолуции претставува добра основа и водич за дефинирање национални политики и стратегии за информациска сигурност, т.е. за дефинирање потребна законска регулатива и правилници со обврзувачко дејство.

Добар пример со скорешен датум на објавување е Декларацијата на ОЕЦД позната под името „Култура на информациската сигурност" (" Culture of Information security- 2002").

Декларацијата дефинира листа на 9 принципи, кои членките на ОЕЦД треба да ги почитуваат и да ги применуваат при изградбата на соодветни национални законски проекти. Намената на декларацијата е земјите-членки да се раководат со основните принципи при разработката и при воведувањето специфични мерки и регулативи во своите држави.

Основните ОЕЦД Принципи (“OECD Principles”)се :

Awareness - Свест за информацискатa „небезбедност”
Учесниците треба да станат свесни за потребата од сигурност на информациските системи и што треба да направат таа да се зголеми.

Responsibility - Одговорност
СИТЕ учесници се одговорни за сигурноста на информациските системи и мрежи.

Response - Реакција
Сите учесници треба да реагираат времено и кооперативно во функција да обезбедат, откријат и да одговорат на секој безбедносен инцидент.

Ethics - Етичност
Учесниците треба да ги почитуваат легитимните права и итереси на останатите.

Democracy - Демократичност
Безбедноста на информациските системи и мрежи не треба да биде во спротивност со ОСНОВНИТЕ вредности на демократичното општество.

Risk assessment - Оцена на ризици од информациски „напади”
Учесниците треба да прават идентификација и оцена на ризиците.

Security design and implementation - (Проектирање системи за сигурност на информациите)
Учесниците треба да ја обезбедат сигурноста на информациските системи со воведување ефикасен управувачки систем.

Security management - (Управување со системот за сигурност)
Учесниците треба да усвојат комплетен и прецизен систем за управување со сигурност на информациските системи.

Re-Assessment -(Редовни ревизии и подобрување на системите за информациска сигурност)
Учесниците треба да прават редовна ревизија на постоечкиот систем за сигурност на информации и да спроведат соодветни подобрувања во безбедносните политики, практики и мерки.

Во поглед на информативната сигурност, денес може да се идентификуваат повеќе различни иницијативи за изработка и за заживување на еден унфициран стандард за имплементација, но и за следење на нивото на заштита на информацијата. Некои од нив се почнати како национални стандарди, кои потоа се дополнително објавени и прифатени како меѓународни, како, на пример, Британскиот стандард - BS 7779, кој е промовиран како меѓународен под името ISO17799, односно ISO27001. Овој стандард е етаблиран како светски признаена и позната методологија, односно рамка за имплементација на систем за управување со сигурноста на информациските системи (ISMS).

Во светот постојат и многу други помалку или повеќе успешни, потврдени и признаени стандарди класифицирани во зависност од начинот на кој ги третираат прашањата на сигурноста, односно се користат како мерка за евалуација и процена на степенот на сигурноста.

Во основа секое регулаторно барање е спецификација на минимум прифатлива имплементација на контроли и мерки за управување на ризиците во рамките на информациските системи (детекција, превенеција и/или корекција). Притоа, овие барања може да бидат на ниво на:

- Препорака (discretionary) базирани на принципот на „би требало" (should) или
- Задолжителни (mandatary) базирани на принципот „ќе" (shall), што значи дека станува збор за препораки кои мора да бидат имплементирани бидејќи се наложени од страна на законски акт или друга повелба од страна на легални субјекти.

Според тоа, може да се препознаат два основни главни правци во развојот на стандардите, поврзани со сигурноста, како што следува:

- Стандарди што ги третираат прашањата на сигурност на едно општо или генерално ниво (ISO 17799/ISO 27001, Common Criteria ISO 1543, UTSEC, ITIL)
- Специјализирани, односно задолжителни барања преточени во конкретни законски стандарди за одредена област, односно деловен процес/индустрија (SOX, HIPAA, Graham Bel).

Во продолжение следи описот на некои од најважните регулаторни препораки, односно стандарди, кои припаѓаат на двете посочени групи - генерални и специфични стандарди.

Општи стандарди

- ISO **27001** (ISO **17799**) / BS **7799** - во моментов, можеби е најраспостранетиот и најпознатиот стандард што се однесува на информативната сигурност, публикуван од страна на меѓународната организација за стандардизација ISO како меѓународен стандард, иако, всушност, произлегува од еден национален - британскиот BS 7799. Тој претставува водич, односно работна рамка, (анг. framework) со базични препораки за имплемента-

ција и за управување со сигурносните ризици и контроли во рамките на информацискиот систем. ISO 17799 често се користи како генерички термин, кој означува стандард за информативна сигурност, иако во суштина тој се состои од две целини:

- BS ISO/IEC **17799:2005** (BS **7799** Part **1**) *Code of Practice for Information Security*, кој содржи насоки за имплементација на сигурносни контроли по принципот - “you should”.
- ***BS ISO/IEC 27001:2005*** (BS **7799-2**) *Information technology, Security techniques Information security management systems — Requirements* и се користи како мерка/водич при проценатa, односно проверката на ефикасноста на имплементираните контроли, односно претставува сертификациски стандард по принципот - “you shell”.

Во моментов, овој стандард е во фаза на ревидирање и на промени, со цел негово консолидирање и усогласување со новите технолошки достигнувања и актуелните ризици. Всушност, се работи за сет од стандарди познати како ISO 27000 серија, која ги содржи следниве конкретни реализации:

- ISO 27000 - поимник за користени дефиниции во ISO 27000 сериите
- ISO/IEC 27002 - предлог за замена на ISO 17799, односно BS 7799 part 1
- ISO/IEC 27003 - нов водич за имплементација на ISMS
- ISO/IEC 27005 - предлог за имплементација на системот за управување со ризиците
- ISO/IEC 27006 - водичи за процесот на сертификација

- TCSEC Trusted Computer Security Evaluation Criteria - познат уште како “Orange Book”, објавен од страна на Министерството за одбрана на САД уште во 1985.

- ITSEC Information Technology Security Evaluation Criteria - усвоен од страна на Велика Британија, Германија, Франција и на Холандија во текот на 80-те години на минатиот век како обид да се хармонизираат и усогласат нивните напори за сигурноста на информациските системи.

- The Common Criteria - практично претставува обид за обединување на европскиот - ITSEC и северноамериканските критериуми: TSEC, CTCPEC (Canadian Criteria) во една стандардна и усогласена работна рамка и методологија за работа. Таа е објавена и прифатена од страна на меѓународната организација за стандардизација како ISO 15408. Со други зборови, Common Crtieria обезбедува разумно ниво на осигурување за тоа дека процесите, нивната спецификација, евалуација и изведба се во согласност со препораките и контролите за обезедување заштита и интегритет на информациите.

- ISO **13335** - IT security management, како сет насоки и препораки за имплементација, пред сè, на технички контролни мерки. Тој содржи серии од стандарди, како што следува:

- ISO 13335-1:2004 “Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management”. ((ISO/IEC TR 13335 parts 1 and 2 were combined into the revised ISO/IEC 13335-1: 2004)
- ISO TR 13335-3:1998 “Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security”.
- ISO TR 13335-4:2000
- ISO TR 13335-5:2001 (ISO/IEC 18028-1)

- ITIL – IT Infrastructure Library предложен и изработен од страна на United Kingdom’s Office of Government Commerce (OGC). Се работи, пред сè, за препораки што ги регулираат и воспоставуваат правилата и насоките за имплементација на системот за управување со процесите во информациските системи, со цел да се обезбеди нивна ефикасност и ефективност. Иако во фокусот на овој стандард не е сигурноста на информацијата, сепак, од исклучителна важност е неговата примена, бидејќи обезбедува солидна основа за имплементација на системот за управување со сигурноста. ITIL е објавен и прифатен како меѓународен стандард - ISO 20000 (BS 15000) и практично се состои од:
  - ISO/IEC **20000** Part **1:2005** “Information technology service management. Specification for Service Management.”
  - ISO/IEC **20000** Part **2**:2005 “Information technology service management. Code of Practice for Service Management.”

- CobiT, Control Objectives for Information and related Technology изработен и предложен од страна на Information Systems Audit and Control Association (ISACA) - претставува работна рамка за имплементација на постапки и методологија за процена на адекватноста и целисходноста на преземените контроли и мерки во рамките на информациските систем.

- RFC-**2196** Site Security Handbook – публицирана со цел да се обезбедат минимум препораки и контроли, кои мора да се специфицираат и исполнат за сите системи што се однесуваат на поврзувањето и користењето интернет како светска глобална компјутерска мрежа.

- Federal Information Processing Standards Publications (FIPS PUBS), USA кои содржат конкретни правила и контролни мерки и кои сите федерални институции во САД мора да ги применат, со цел да обезбедат сигурен информациски систем. Овие FIPS стандарди произлегуваат од законската повелба Federal Information Security Management Act of **2002** (“FISMA“) усвоена во 2002.

- GASSP - Generally Accepted System Security Principles (Version **2.0**) **предложена од** International Information Security Foundation

Специјални стандарди и законски решенија

- HIPAA, Kennedy-Kassebaum Health Insurance and Portability Accountability Act САД 1996 (дополнет во 2000); се однесува на прашањата што ја покриваат заштитата на информацијата во здравствените институции, обезбедувајќи приватност и доверливост на информацискиот систем. Тој е прифатен и потврден како defacto меѓународен светски стандард за заштита на информациите во здравството и во социјалноосигурителните компании и установи.

- The Gramm-Leach-Bliley Financial Services Modernization Act, САД 1999; се однесува на заштитата на информациските системи во финансиските институции: банките, финансиските пазари и берзите за тргување со хартии од вредност.

- Sarbanes-Oxley Act of **2002,** односно SOX - Public Company Accounting Reform and Investor Protection Act of 2002, САД; претставува законски акт, кој содржи мерки и контроли што се однесуваат на обезбедување на интегритетот (точноста и комплетноста) на генерирањето на финансиските извештаи, како и обезбедување на расположивоста на сет извештаи до менаџментот - Management Information System-MIS системот, со цел да биде достапен во моментите на носење деловни одлуки. Иако основна цел на овој стандард е точноста и интегритетот на финансиските извештаи, тој нуди серија контролни мерки и прописи во однос на информативната сигурност, како што е сегрегацијата на должности и правото на пристап до информациите. Во денешниот миг на развој на компјутерската, односно информатичката технологија и заживувањето на глобалниот пазар, станува сè поактуелен и значаен, не само во САД, туку и во меѓународните односи и релации на компаниите.

4. АСПЕКТИ НА ИНФОРМАЦИСКАТА СИГУРНОСТ

4.1. Државни институции

Државните институции како креатор, сопственик и корисник на информациите и информациско-комуникациските средства.

Државните институции претставуваат најголем сегмент на имателi, корисници и креатори на информациите во секоја држава.

Според Законот за класифицирани информации на Република Македонија, термините „информација” и „документ” ги дефинира на следниот начин:

- „**Информација**” е сознание кое може да биде пренесено во која било форма.
- „**Документ**” е секој запис на информацијата без оглед на нејзината физичка форма или карактеристики, вклучувајќи, без ограничување, пишан или печатен текст, карти, шеми, фотографии, слики, цртежи, гравури, скици, работни материјали, индиго или лента или репродукции со помош на какви било средства или процес, како и звучни, гласовни, магнетски или електронски, оптички или видеоснимки во која било форма, како и преносliва опрема за автоматска обработка на податоци со вградени или преносливи мемории за складирање податоци во дигитална форма.

Исто така, законот ги обврзува сите правни и физички лица со информациите да се однесуваат на законски начин и да се обезбедат мерки за спречување на неовластено користење.

За таа цел, секоја институција треба да обезбеди мерки за информациска сигурност, со специјален нагласок на класификација на информациите, овластување за нивно користење, лични сертификати и особени административно- организациски мерки (безбеден простор, безбедна опрема).

За доследна примена на законот и начинот на неговото спроведување постои Дирекција за класифицирани информации со соодветен инспекциски орган.

За државните институции, како „доминантен" креатор, сопственик и корисник на информациите, постојат две актуелни теми кои се директно поврзани со прифаќањето на концептот на „Култура на информацискатa сигурност:

- Е-Влада и
- Сигурност на националните информатички инфраструктури

Е-Влада има повеќе аспекти во кои е вклучена информацискатa сигурност. Тоа се пред сè:

- Сигурност и обезбедување услови за непрекинато работење во редовни и вонредни услови на сите битни интерни активности што се одвиваат во институцијата
- Сигурност во соработката и размена на информации со други државни институции („интероперабилност")
- Сигурност во соработката и размена на информации со други меѓународни институции (прекугранична интероперабилност)
- Сигурност во реализацијата на конвенционалните услуги како и е-услугите за граѓаните и стопанските субјекти (автентичност - проверка на идентитет, достапност како и точност)
- Безбедни „партнери" за функционирањето на државната институција (комуникациски услуги, добавувачи на електрична енергија, добавувачи на ИТ-опрема, апликации и други ИТ-сервиси).

Сигурноста на националните критични информатички инфраструктури е нова обрска на државата да обезбеди непрекинато работење на дефинирани национални информациски инфраструктури, каде што информатичкиот фактор има значајна улога. Информатичкото општество директно зависи од расположивоста на националните критични информациски инфраструктурни мрежи и од интернет.

Оваа инфраструктура е ранлива, како од класичните видови напади (тероризам, DoS[4]), така и од ненамерни инциденти (човечки фактор, технички фактор).

[4] Denial of service attacks

Што може да прави државата?

А. Изработка и донесување потребна законска рамка за подобрена информациска сигурност

Таа „рамка” треба да содржи пред сè, а и во согласност со постоечките меѓународни декларации и конвенции/директори:

- Национална политика и стратегија за информациска сигурност
- Измена на закони за битни сфери кои се специјално чувствителни на информацискатa небезбедност (електронска комерција, е-Влада, финансиски систем, здравствен систем,...)
- Акциски планови за секоја државна институција за спроведување минимални информациско-безбедносни мерки со придружен национален буџет
- Обезбедување организациска поддршка во државните институции и јавните претпријатија, иматели на информации, на мерките за инфромациска сигурност (функција/сектор за информациска сигурност, одговорно лице – CISO Chief Information Security Officer)

Б. Активности на национално ниво

- Покренување акции за зголемување на свеста за постоењето и важноста на информацискатa небезбедност, ризиците поврзани со тоа и потребата за подготвеност за заштита и брзо закрепнување во случај на реализиран информациски инцидент / напад.

  Субјекти за кои би биле наменети предложените акции се :
  - Граѓаните и нивните домаќинства
  - Институциите од невладиниот сектор
  - Стопанскиот сектор
  - Државните институции, локалната самоуправа и јавните претпријатија
  - Обезбедување соодветна државна организациска инфраструктура за справување со информациските инциденти (Центри за регистрација на информациски инциденти и поддршка)

В. Активности поврзани со образование и со дисеминација на препораките за зголемување на информацискатa сигурност за сите засегнати странки (граѓани, стопански субјекти).

Г. Активности поврзани со учество во меѓународни соработки, проекти и активности за борба против информациските инциденти.

Д. Обезбедување финансиска поддршка и други олеснувачки мерки за зголемување на информацискатa сигурност за сите засегнати странки (граѓани, организации од невладиниот сектор и стопанските организации).

4.2. Локална самоуправа

Единиците на локалната самоуправа се основната „линија на фронтот" за информациска сигурност на граѓаните и на нивните семејства. Реална претпоставка е дека во блиска иднина секое семејство ќе биде приклучено на глобалната интернет-мрежа. Со тоа секој член во општеството ќе ги споделува богатствата што ги овозможува интернет, но, исто така, ќе ги споделува и опасностите, заканите и штетите што се дури и денес неизбежни.

Утре, информацијата дека во текот на годината се појавиле 10.000 вируси, дека 1.000 компјутерски системи биле „нападнати" и блокирани нема веќе да биде приказна што му се случува на некој друг. Мотото на Хемингвеевата прекрасна книга „За кого бијат камбаните" добива ново и актуелно значење.

Информациската безбедност е сечија обврска. Тоа не ја намалува важноста на организираната локална самоуправа таа заштита да ја организира и да ја зајакне. Останува само прашањето – КАКО?

По природа на нештата редоследот на основните прашања би бил:

Зошто е важна ефективна и ефикасна информациска безбедност?

Листата со примери (која во никој случај не е дефинитивна) на информациски инциденти содржи:

- Вашиот омилен ВЕБ-САЈТ е неактивен и недостапен за повеќето корисници
- Комјутерите во Вашата фирма се неупотребливи поради присуство на вируси
- Некој хакер „влегол" во вашиот домашен компјутер, ги „украл" адресите од вашиот електронски адресар и во ваше име дистрибуира штетни пораки на сите ваши пријатели со кои досега сте комуницирале по електронски пат.
- Незадоволен отпуштен вработен го искористил својот пристап до комјутерскиот систем во фирмата во која работел и уништил важни деловни информации

Дури и компјутерите што не се приклучени на интернет може да бидат објект на информациски „напад" . Необезбеден/заштитен компјутер може да биде злоупотребен од неовластен корисник (гостин во вашата канцеларија или во вашиот дом), со тоа што ќе има можност без ваше знаење и дозвола да има пристап до битните ресурси во компјутерот (бази на податоци, уреди за читање), со тоа што ќе користи непроверени и потенцијално опасни игри, програми или цедеа. Непоправливи измени и/или бришење податоци во вашиот личен компјутер е, исто така, можно во случај на негово користење од недобронамерен корисник во ваше отсуство.

Во случај компјутерските системи во единиците на локалната самоуправа - необезбеден систем може да дозволи неовластено бришење или промена на битни информации за граѓаните, катастарот, имотот. Тоа ја прави обврската на единиците на локалната самоуправа да посветуваат внимание на информациската безбедност како НАДЛЕЖНОСТ, а не како опција.

Што значи НЕБЕЗБЕДЕН и НЕЗАШТИТЕН компјутер?

Незаштитен и небезбеден компјутер значи компјутер што НЕМА :

- Инсталирана и РЕГУЛАРНО ОБНОВУВАНА антивирусна заштита и СПАЈВЕР заштита
- Инсталирана хардверско/софтверска заштита од типот на ФАЕРВОЛ, со кој се спречува пристап до интерната мрежа од надворешни корисници на интернет.
- Бекап на битните бази податоци сместен надвор од зградата каде што се наоѓа комјутерскиот систем (можеби на РЕЗЕРВНА локација)
- Вградена заштита на пристап: кориснички имиња и лозинки за пристап и за користење на компјутерскиот систем во целина, на поединечни апликации и/или поединечни бази на податоци
- Нема практика на РЕДОВНО ажурирање апдејти на оперативниот систем

Кои се целите на информациската безбедност во единиците на локалните самоуправи?

Како „чувари” на битни информации за граѓаните, единиците на локалната самоуправа имаат надлежност и обврска за нивно безбедно сместување и користење. Основните акции што треба да ги направат единиците на локалната самоуправа за да обезбедат прифатливо ниво на информациска безбедност се :

- Промоција и градење свест кај граѓаните и вработените за потенцијалните информациски инциденти и оштетувања, т.е. опасности.
- Овозможување тренинг за подобрување на информациската безбедност и исправно користење на комјутерски системи, како за вработените така и за граѓаните (во партнерство со други институции: НВО и бизнис).
- Презентација и информирање за обврските за информациската безбедност кај сите субјекти: локална самоуправа, работни организации, семејства, поединци.
- Систем за информирање на појава на информациски закани (нови вируси) и инструкции за ургентно справување со нив – „прва помош“ преку веб-сајтовите на единицата на локалната самоуправа.
- Градење свест за можност за „невозможно” („Ништо не смее да нè изненади”) и подготовка за „закрепнување” од таквите состојби.

Што МОРА да се направи ?

Основната порака гласи: „Информациската безбедност е СЕЧИЈА обврска!". Тоа не смее да значи - НИЧИЈА!. Секој од нас треба секојдневно да води сметка за безбедноста на компјутерот и за информациите со кои се користи.

Единиците на локалната самоуправа имаат избрани советници, перманентно вработени, привремено вработени и надворешни даватели на услуги како на самата единица, така и на граѓаните.

Со самото вработување и можност/потреба за користење на компјутерскиот систем во единицата на локалната самоуправа секој советник,вработен и надворешен корисник треба да бидат запознати со правилата на безбедно и овластено користење на компјутерските ресурси. Сите надворешни добавувачи на сервиси треба да ги почитуваат тие правила и да одговараат за нивното почитување со т.н. договори за доверливост. Непрекинатиот надзор на користењето на компјутерскиот систем треба да биде редовна практика.

Информациската безбедност е тука за да остане. Целиот процес почнува со донесување политика за информациската безбедност и потоа се надградува со „добри безбедносни" постапки и процедури, кои постојано се надградуваат. Притоа редовно се следи и се подобрува системот на правата и обврските за информациската безбедност.

Десет принципи за информациска безбедност

1. Назначете ОДГОВОРНО лице за информациска безбедност во единицата на локалната самоуправа.
2. Научете како да осознаете дека имате информациско- безбедносен проблем, закана или напад.
3. Научете и подгответе се да се справувате со појавени информациски инциденти.
4. Физички обезбедете ги информациските ресурси (компјутери, податоци, комуникации).
5. Осигурајте ги основните и битните информациски ресурси (бекап, резервна опрема, резервна локација).
6. Дозволете пристап до компјутерите ИСКЛУЧИВО на овластени лица и обезбедете заштита од неовластени корисници.
7. Обезбедете ги информациите (криптирање).
8. Постојан тренинг.
9. Дефинирајте ја политиката на информациската безбедност и политика за дозволена употреба на компјутери и информации.
10. Обезбедете средства, ресурси и постапки за „регулирано" уништување на постоечките, а сега непотребни информации и компјутери.

4.3. Банки

Банките по својата природа на работа во денешниов миг од технолошкиот развој припаѓаат во групата на таканаречените „computer depends organizations”. Со други зборови, практично ИКТ е стожерот околу кој се гради и имплементира целокупната бизнис-политика и стратегија. Имајќи ја предвид комплексноста и чувствителноста на сервисите и услугите што ги нудат банките, од исклучителна важност се прашањата поврзани со сигурноста и со заштитата на информациите да се третираат и разрешуваат на еден систематски и сеопфатен начин.

За таа цел, во декември 2003 година, Советот на Народна банка на Република Македонија донесе одлука за дефинирање на стандардите за подготвување и за спроведување на сигурноста на информацискиот систем на банките („Службен весник” на РМ бр. 77/2003). Врз основа на таа одлука, во јуни 2005, НБРМ издаде супервизорски циркулар, со кој подетално се определуваат стандардите за управување и контрола на ризиците значајни од аспект на сигурноста на информацискиот систем, како и стандардите за обезбедување континуитет во работењето на банките. При изработката на оваа одлука, како и при изработката на овој циркулар, се користени препораките и насоките содржани во Меѓународниот стандард за управување со сигурноста на информацискиот систем (***BS7799-2:2002,*** односно ***ISO/IEC17799:2000***) и базелскиот документ за управување со оперативниот ризик.

Примената на овие стандарди ќе обезбеди зголемена безбедност на информациите што се чуваат во информацискиот систем и повисок степен на интегритет на податоците при различни видови обработки. Неопходно е информацискиот систем на банките да им е расположив, односно достапен на вработените и на коминтентите за непречено одвивање на банкарските операции, како и на органите на управување за носење прудентни одлуки, во рамките на своите деловни потреби и дозволени авторизации. Овој циркулар нема амбиции да ги покрие сите аспекти на управување со сигурноста на информацискиот систем, туку, пред сè, да служи како насока во дефинирањето и воспоставувањето адекватни стандарди за обезбедување сигурност на информацискиот систем, дефинирање на правата и одговорностите на лицата што се носители на сигурноста на информацискиот систем и врз таа основа да овозможи следење на утврдените законски норми за сигурноста на информацискиот систем од страна на банките во Република Македонија.

Ефективното управување со информатичката технологија е од посебно значење за употребата на новите услуги и технологии во остварувањето на стратегиските цели на банката. Информативната технологија претставува интегрален и централен дел од процесот на извршување на најголемиот број банкарски операции. Управувањето со инофрмативната технологија не претставува само управување со трошоците што се направени при извршувањето на банкарските операции и контролата на нивното спроведување,

бидејќи напредокот во технологијата може да резултира со понуда на нови сервиси и производи, кои можат да значат зголемување на изложеноста на ризиците на банката. Според овие препораки, основата за ефикасен и ефективен систем за управување со сигурноста во банките е изработката на **политика за сигурност на информацискиот систем.** Политиката за сигурност на информацискиот систем претставува **темел** на градењето на процесот на информативната сигурност. Политиката треба да ја дефинира методологијата што ќе се применува за процена на ризикот и големината на прифатливиот ризик за менаџментот на банката. Во политиката треба да стои и кои се соодветните документи што треба дополнително да се креираат, како што се: процедури, стандарди и упатства, а ќе придонесат за подетално, постепено разработување на сите аспекти за обезбедување посигурен и непрекинат информациски систем.

Како посебен дел во регулативата за сигурноста на информацискиот систем е соодветната заштита на личните податоци, која банката ја обезбедува за своите комитенти, вработени и сите други субјекти на личните податоци (физички лица на кои се однесуваат обработените податоци), чии лични податоци по која било основа (согласност, договор и др.) и на кој било начин (автоматизирано или рачно) се обработуваат во банката. Документите, податоците и информациите што се стекнати при вршењето банкарски и други финансиски активности за поединечни лица и соодветни трансакции и депозити (штедни влогови) што ги поседуваат претставуваат **банкарска тајна,** која банката е должна да ја заштити и чува. Исклучок од ова претставува ситуацијата кога:

- со закон е пропишано објавување на податоците и информациите и
- ако комитентот дал писмена согласност за откривање на податоците.

Покрај барањата за имплементација на контроли и мерки, новина е тоа што како резултат на споменатата одлука се формира и се воспоставува нова задолжителна функција во рамките на банките наречена: **Одговорен за сигурноста на информацискиот систем (ОСИС).** Ова лице е од витално значење, бидејќи е замислена како носител на сите активности поврзани со сигурноста, односно треба да врши процена на ризиците, анализа на веројатноста од појава на заканите, да предлага унапредување на политиките и процедурите за информативна сигурност. Основните функции на ОСИС се како што следува:

- Изработка на политика за сигурност и воспоставување критериуми за евалуација на ризиците и посакуваното ниво на сигурност во информацискиот систем.
- ефективно функционирање на процесот на информативна сигурност на ниво на целата банка.
- набљудување на нарушувањата на политиките и процедурите и учество во тестирањата на ефективноста на имплементираните контроли.
- Управување со сигурносните инциденти и координација на менаџментот, со цел преземање координирана акција за заштита на банката од можни финансиски загуби.

4.4. Информациска сигурност за бизнис-секторот

Многу мали и средни фирми веруваат дека тие се неатрактивни за напади врз нивната ИКТ-инфраструктура или за самите податоци. Секоја фирма може да биде предмет на информациски напад. Според една од анкетите, вирусот „My Doom” (еден од многуте) нападнал една третина од малите фирми во САД минатата година.

Малите фирми обично оперираат со помали профити и затоа нивните менаџери треба да бидат попретпазливи во обезбедувањето на тие не премногу големи профити. Губењето на финансиската документација ќе влијае врз функционирањето на целата фирма. Резултат на тоа би било нереализиран приход, зголемени камати на неплатени сметки, дополнителни казни поради доцнење на уплата на даночните обврски.

Следниве прашања ќе Ви помогнат да направите евалуација на Вашата политика за информациска сигурност:

1. Колку ќе Ве чини „поправката” на оштетените податоци и програми?
2. Колку ќе Ве чини нивна замена, т.е. набавка на нови програми и регенерирање на оштетените или загубените податоци?
3. Колкава е штетата поради изгубен „имиџ” на сигурен деловен партнер?
4. Колку ќе Ве чини „застојот” т.е. неработењето додека не профункционира вашиот компјутерски систем?

Дали овој ВОДИЧ е применлив и врз мојот вид фирма?

Едно од можните објаснувања зошто малите фирми се поизложени на информациски напади, отколку големите фирми е токму нивната големина. Големата фирма може да си дозволи да има организациска единица, која управува со компјутерските функции и во тој систем може да има и единица за информациска сигурност, која редовно води сметка за информациската безбедност. Малите фирми ретко може да си дозволат постоење на специјална работна единица задолжена за информациска сигурност на фирмата.

Токму овој факт отвора можност специфични професионални здруженија на мали фирми да имаат „заеднички” сервисен центар за информациска сигурност, кој би нудел безбедносни сервиси на своите членки.

Многу информациски напади се упатени кон помали фирми. „Напаѓачот" едноставно испраќа огромен број пораки кон СИТЕ и таму каде што нема да наиде на заштита, го почнува својот малициозен напад. Ако Вашата фирма нема антивирусна заштита, "firewalls", а има безбедносно несовесни корисници, тогаш не само што има можност за штета во вашата фирма, туку вашиот компјутерски систем со ПРЕПРАЌАЊЕ на штетните пораки е извор на проблеми во голем број други фирми.

Необезбеденост на Вашиот систем:
1. Ве прави идеална и лесна жртва
2. Ве прави „соучесник" во штетните активности и посредник во информациските криминал

Сите што користат интернет ИМААТ ОБВРСКА И ОДГОВОРНОСТ да помогнат во градење на „Култура на информациска безбедност" со која и со што ќе придонесат во градење безбеден економски простор и заштита на сите економски субјекти: партнери и купувачи.

Затоа наместо „{тедење", попаметно е „рационално" инвестирање во информациска сигурност. Затоа почнете со изработка на план за информациска сигурност и стратегија за негово спроведување. Таа постапка е идентична со постапката за изработка на маркетинг- план на вашата фирма.

Чекори во планот за информациска сигурност :
1. направете анализа и попис на тоа што е „информациски" битно за Вашето работење: кои податоци, кои програми, која опрема?
2. направете процена за можиот ризик да се случи нешто лошо.
3. Пресметајте колкава ќе биде штетата ако тоа НАВИСТИНА се случи.
4. Оценете колкав дел од буџетот можете да употребите за информациската сигурност.
5. Направете ПРИОРИТЕТНА листа (според важноста и според ризичноста) на информациски „објекти" (податоци, програми, опрема) и почнете со реализација на безбедносните мерки, една по една од врвот на листата, па надолу.

Места каде што можете да добиете помош поврзана со информациската сигурност :
1. Замолете го испорачателот на вашата компјутерска опрема и програми редовно да ве информира за новините во заштитните мерки, кои се препорачани од производителите на инормациската опрема и програмите.
2. Во случај на идентификуван информациски „напад" – појава на вирус, информирајте го Вашиот интернет- провајдер и побарајте совет како да се справите со новопојавениот вирус.

3. Во случај на предизвикана бизнис-штета од посериозни размери пријавето го тоа во Министерството за внатрешни работи. Тие имаат високо специјализиран орган за истражување на компјутерскиот криминал и се способни да Ви помогнат. Инаку, според кривичниот законик тоа е и ваша обврска.
4. На интернет постојат специјализирани „дискусиони бази”, каде што луѓе како Вас расправаат за проблемите што ги имаат, како ги решаваат и предлагаат заеднички акции за справување со ваков тип проблеми.
5. Ангажирајте консултант за информациска сигурност.

5. КОМПЈУТЕРСКИОТ КРИМИНАЛ КАКО ОСНОВА ЗА НАРУШУВАЊЕ НА ИНФОРМАЦИСКАТА СИГУРНОСТ И ПРИВАТНОСТА

Разновидните форми на непосредна примена на компјутерот во сите области на животот не останаа незабележани од несовесните поединци, кои не бираат средства и начин противправно за себе или за друг да стекнат некаква имотна корист.

Компјутерот стана и средство за вршење разни облици на недозволени и општествено опасни активности. Имено, под поимот компјутерски криминал се опфатени сите оние облици и форми на кривични дела поврзани со злоупотребата на компјутерот и информатичките системи, воопшто.

Главни обележја на овој вид криминалитет се:

- општествено опасни, противправни однесувања за кои законот пропишува кривични санкции;
- специфичен начин и средство на вршење на кривично дело со помош или со посредство на компјутер;
- посебен објект на заштита, безбедност на компјутерските податоци или информатички системи во поединечни сегменти или во целост;
- намерата на сторителот за себе или за друг да прибави некаква корист (имотна или неимотна) или на друг да му предизвика штета;

Интернет-мрежата сега е достапна во повеќе од 200 земји и криминалните дела можат да бидат извршени преку оваа мрежа од која било држава, жртвите, исто така, можат да бидат каде било, сторителот, исто така, лесно може да го скрие својот идентитет, дејствувајќи од земји каде што тој не е државјанин, туку престојува само кратко во нив.

Доказите за овие дејствија, исто така, не мора да бидат на една локација, туку тие можат да бидат на повеќе локации.

Можноста да се следат интернет-комуникациите од различни компјутерски мрежи и локации каде што постојат различни јурисдикции и надлежности е критичин елемент за превенција, истражување и за гонење на компјутерскиот криминал.

Поради ова и се покренати различни интернационални иницијативи и конвенции за широка меѓународна соработка во сузбивањето на овој вид криминал како Конвенцијата за компјутерски криминал на Советот на Европа (Будимпешта 2001).

Појавни облици и начини на извршување на кривичните дела од областа на компјутерскиот криминал:

- компјутерска измама
- финансиски кражби и злоупотреби
- фалсификување податоци и документи
- компјутерски вандализам
- изработка и употреба на компјутерски вируси
- компјутерска саботажа и шпионажа
- хакерство

Компјутерската измама е кривично дело што го врши одредено лице со внесување одредени неточни податоци или невнесување одреден важен податок, со цел тоа да влијае врз резултатот на електронската обработка или на преносот на податоците и така за себе или за друг противправно да прибави одредена имотна корист или да нанесе штета на друг.

Финансиските кражби и злоупотреби со помош на компјутер се едни од најчестите компјутерски кривични дела и се однесуваат на злоупотребата на кредитните картички, кои пак се едни од најмодерните платежни средства и на разни навлегувања во заштитените системи и правење недозволени финансиски трансакции.

Сегашниот степен на развој на компјутерите дозволува дигитализација и менување на содржината на разни акти и документи што се користат при правниот сообраќај, како и на фалсификување податоци кои се во електронска форма. Дури честопати постојат и обиди за фалсификување на банкноти со помош на компјутер и периферни уреди, како скенер и печатач, чии технички можности денеска се на високо ниво, дури и кај уредите за широка потрошувачка.

Под компјутерски вандализам се подразбира намерно навлегување во туѓи компјутери и заштитени компјутерски системи и бришење и уништување податоци без некоја посебна цел, туку само заради предизвикување одредена штета кај системите што се објект на напад во поглед на нивното правилно функционирање.

Софтверот, односно програмите се едни од најмоќните оружја на сајбер-криминалците. Под поимот компјутерски вируси се мисли на програми, кои несовесни поединци ги пишуваат за да нанесат што поголема штета на многу компјутери врзани во мрежа, како на пример на глобалната интернет-мрежа. Нивни основни одлики се:

- Се копираат самите себеси на секој компјутер со кој ќе дојдат во контакт.
- Не се забележливи, т.е. најчесто се невидливи за корисникот на компјутерот, посебно ако на компјутерот не е инсталиран специјализиран софтвер за нивна детекција.
- Автоматски извршуваат одредени команди, како бришење корисни податоци на компјутерот на жртвата или, пак, ги испраќаат податоците на одредена друга локација на мрежата без знаење на сопственикот на компјутерот.

Покрај хакерите и групите што тие ги организираат за неовластено навлегување во заштитените системи, во денешно време постојат и специјализирани тајни владини служби, кои преку навлегување во компјутерскиот систем на другите држави прибавуваат податоци од разузнавачка природа. Така, под поимот компјутерска шпионажа може да се дефинира еден од најмодерните облици на разузнавање, но, исто така, постои и индустриска шпионажа, која е од комерцијална природа.

Компјутерска саботажа имаме во случај кога некој ќе уништи, избрише, промени, прикрие или на друг начин ќе онеспособи податок, програм или ќе го оштети компјутерот, кој е од значење за државен орган, институција, јавна служба.

Сајбер-криминалците или популарно наречени хакери се по правило лица со посебни стручни и практични знаења и вештини од доменот на високата информатичка технологија, кои своите знаења ги користат за нанесување штети на одредени заштитени системи. Хакерството како модерен феномен произлегува од техничкиот предизвик да се пробие заштитата на одреден информатички систем и да се навлезе во него. Колку е заштитата посилна, толку е предизвикот поголем. Овие кривични дела се вршат прикриено без просторна поврзаност меѓу сторителот и жртвата и по правило тешко се докажуваат, т.е. остануваат во темната бројка на криминалитетот. Честопати дури ни администраторите на мрежните системи не можат да забележат неовластено навлегување во системот од страна на хакер, сè додека системот не претрпи некоја штета.

5.1 Законска регулатива за компјутерскиот криминал кај нас

Член 251 од КЗ на (навлегување во комјутерски систем) сл. весник бр.37/1996 год.

Кај нас ова кривично дело е внесено во КЗ во 1996 година и од тогаш па наваму се применува овој член во практиката. Спаѓа во глава 23 кривични дела против имотот од КЗ на РМ.

Сега овој член е проширен и со повеќе потчленови што се однесуваат на изработка и внесување компјутерски вируси (чл.251а), компјутерска измама (чл.251б).

КОИ СЕ НАЈПОЗНАТИТЕ СВЕТСКИ ХАКЕРИ

Кевин Митник алијас Кондор

Легенда на хакерството во светот е секако Кевин Митник со псевдоним Кондор и претставува култен херој на сајбер-просторот како инспирација за новите хакери што го учат занаетот. Првото обвинение против него е покренато уште во 1995 година поради фалсификување 20.000 броеви на кредитни картички и поради неовластено навлегување во системите на компаниите Моторола, Сан микросистемс, Нокиа, Фуџитсу и многу други. Штетата што ја предизвикал е проценета на 80 милиони долари. естопати навлегувал и во системите на државните институции на САД, како системот на северноамериканската команда за одбрана НОРАД уште во 1983 година, НАСА, па дури и на ФБИ, од чија страна е и уапсен во 1992 година. Последната затворска казна му беше 5 години и 2 години забрана за пристап на интернет. Долго време бил меѓу 10-те најбарани криминалци на сајтот на ФБИ. Инспирација е за неколку холивудски филмови, како „Воени игри", „Такедоун", „Хакери" и други.

Владимир Левин

Русин, по потекло од Санкт Петербург, кој успеал да навлезе во системот на Citybank во САД, во 1994 година и да извлече 10 милиони долари. Ова е неговиот најголем потфат, но е откриен и е уапсен, а Citybank успева да го поврати најголемиот дел од сумата.

5.2. Статистички податоци за влијанието на компјутерскиот криминал врз имплементацијата на новите технологии во светот

Постојат многу различни статистички податоци за влијанието на компјутерскиот криминал врз комуникациите, економијата, криминалитетот, сигурноста итн. Критериумите по кои тие се собирани се, исто така, многу различни во зависност од изворот и на овие статистики треба да им се пристапува со доза на резерва.

Во секој случај, темната бројка кај овој вид криминал е огромна од неколку причини:

1. Просторната распространетост: на пример, сторителот може да биде во една земја , серверот, кој го напаѓа, во друга , а жртвата или последиците во трета. Во ваков случај, собирањето на доказите е многу тешко од аспект на различни правни системи, јурисдикции итн.

2. Жртвите на овие дела честопати не ги пријавуваат овие дела дури и кога се значително оштетени поради стравот од губење на клиентите. На пример, која банка ќе пријави дека нејзиниот платежен систем е пробиен од хакери? Веќе другиот ден многу клиенти ќе ги затворат своите сметки во таа банка.

3. Недоволна организациска поставеност и техничка опременост на органите надлежни за прогон на овој криминал. Секоја држава со оглед на ширењето на употребата на компјутери и интернет- мрежата треба да состави тимови за борба со компјутерскиот криминал, во кои обучени професионалци со соодветна опрема ќе бидат во состојба да ги откријат и да ги докажат пред судот овие дела.

По некои истражувања, само 12 отсто од компјутерскиот криминал станува познат на јавноста или на органите за прогон.

5.3. Економски аспекти на штетите предизвикани од компјутерскиот криминал на глобално ниво

Денес се знае дека компјутерскиот криминал е причина за загуби што се изразуваат во милиони долари во глобалната економија. Многу загубени милиони ќе останат неоткриени. Во иднина билиони долари ќе бидат украдени, повеќето од нив незабележително од главниот криминалец на 21 век - компјутерскиот престапник. Ситуацијата е уште полоша поради фактот дека секој човек кој е компјутерски писмен може да стане компјутерски криминалец. Овој криминал ќе остане виртуелен по својата природа, појавувајќи се најчесто на интернет и оставајќи ги единствените траги зад себе - „електронските” траги и докази.

Вложувањата во електронската сигурност, која со напредокот на технологијата бара сè поголеми инвестиции и инфраструктури, секако прави големо оптоварување во расходите на секоја сериозна институција или компанија, на која заштитата на податоците и е од голема важност. Вработувањето стручен кадар од областа на информатичката сигурност е, исто така, од голема важност.

Истражувањата и развојот на оперативните системи и софтверот во поглед на нивната сигурност, исто така, бара дополнителни инвестиции и ресурси.

Континуираното следење на сигурносните технолошки трендови и имплементацијата на најновите решенија, кои ќе гарантираат одредена доза сигурност е обврска за секоја организација, чии податоци, комуникации или трансакции се објект на заштита.

5.4. Заштита и енкрипција на интернет-комуникациите - технички аспекти

За да се заштити приватноста на податоците што не смеат да бидат јавно видливи или достапни, а кои се разменуваат на глобалната мрежа, тие мора да бидат заштитени или енкриптирани.

Ова подразбира примена на многу технологии за заштита на податоците при пренос низ мрежата, како заштита со разни шеми на енкрипција, заштита со лозинки, заштита по пат на јавен клуч итн.

Нормално е дека податоците што се заштитени на овој начин претставуваат некаква вредност и се цел на сајбер-криминалците, кои сакаат да дојдат до нив за да ги злоупотребат. Тие со целото свое техничко знаење се трудат да ја пробијат најновата шема на енкрипција, најновиот систем на заштита на некоја банка (firewall), да го украдат најновиот скап софтвер и со тоа да извлечат некаква материјална корист или да ја докажат својата техничка супериорност. Организациите, своите информатички системи поврзани во мрежи и податоците мора да ги чуваат од напад како однадвор, така и однатре. Честопати и самите вработени што работат на овие системи вршат злоупотреба на знаењата што ги имаат за конкретниот систем, правејќи кривични дела за да стекнат некаква противправна корист.

За да се обезбеди ефикасна заштита на податоците, организациите мора да се фокусираат на технолошките трендови и процеси, но и на човечкиот фактор. Тие мора да ги едуцираат своите вработени за примена на сигурносните техники и процедури, развиени низ планирање за начинот на постапување со чувствителните податоци, записи или трансакции.

Освен тоа, тие мора и да ја имплементираат денешната робусна сигурносна технологија како заштитните „ѕидови" - firewalls, антивирусниот софтвер, алатки за детекција на напад врз мрежите, напредни алгоритми за енкрипција, автентификација итн.

Имплементацијата во секоја компанија (владин и невладин сектор) на меѓународно воспоставените стандарди за ИТ-сигурност секако дека се основен предуслов за успешно функционирање на ИТ- системите.

Технологијата отиде дотаму што некои производители на хардвер, како процесори (CPU), чип-сетови почнаа со имплементација на хардверска поддршка во процесорите за заштита од вируси или хардверски вграден firewall во чип-сетовите.

5.5. Заклучок и препораки

Еден од приоритетите за пристап кон членство во ЕУ секако е брзото усогласување на нашето законодавство со соодветните европски законодавства.

Затоа брзата имплементација на директивите на Советот на Европа од сферата на компјутерскиот криминал мора да бидат завршени што поскоро.

При донесување закони и подзаконски акти во согласност со директивите на Советот на Европа од сферата на компјутерскиот криминал секако треба да се оформат стручни тимови, во чиј состав, покрај експертите од законодавната сфера, треба да бидат вклучени и ИТ-експерти што ќе им укажат на правните екперти што недостига во нашето законодавство (од областа на кривичните дела што го опфаќаат компјутерскиот криминал) за тоа да биде усогласено со Европските законодавства.

Навистина, во нашиот КЗ има многу малку членови за да се опфатат сите појавни облици и трендови на компјутерскиот криминал во моментов.

За жал, компјутерскиот криминал е во забележителен пораст во РМ.

Посебно во овие тимови треба да бидат присутни екперти од областа на ИТ-сигурност, кои знаат како да се имплементираат сите стандарди за ИТ-сигурност, како во институциите, така и во законодавството.

Подигањето на јавната свест за опасностите што демнат при користењето на новите технологии мора да биде од страна на сите субјекти одговорни за заштита на граѓаните од разни облици на измами и злоупотреби на нивната приватност при користењето на новите технологии.

Тука најважна улога треба да одиграат секако банките како директни провајдери на овие услуги, но и јавните институции, медиумите и невладините организации преку издавање информативни брошури и други начини на јавно информирање.

Посебно, со наглиот продор на користењето разни типови платежни картички во РМ се зголемуваат и опасностите од разни злоупотреби од несовесни поедници, кои мора навремено да се спречат за да се стекне доверба во користењето на овие технологии кај сите корисници на овие услуги, како и да се подигне рејтингот на РМ при работењето со платежните картички преку интернет.

6. РЕФЕРЕНЦИ

- *www.enisa.europa.eu - The European Network and Information Security Agency, ENISA*
- *www.europa.eu.int/information_society - Europe's Information Society*
- www.isc2.org – *The International Information Systems Security Certification Consortium (CISSP - Certified Information Systems Security Professional)*
- www.issa.org – *Information Systems Security Association*
- www.isaca.org - *Information Systems Audit and Control Association ^ Foundation*
- www.sans.org – *SysAdmin; Audit; Network; Security*
- *www.cert.org – Computer Emergency Response Team*
- *www.nist.gov - USA, National Institute of Standards and Technology*
- www.gocsi.com – *Computer Security Institute (CSI/FBI survay)*
- *www.cisspcom – Portal for CISSP*
- *www.securityforum.org – Independent athority on Information Security*
- www.xisec.com – *ISMS International User Group*
- www.securitydocs.com/Policies - *Template for Security Policy*
- *www.nbrm.gov.mkwebstorage/files - Циркулар за сигурност на информацискиот систем на банките*
- *www.masit.org.mk – Македонска асоцијација за информатичка технологија*
- *www.e-gov.org.mk – USAID проект за развој на е-општество во Р.М.*
- *www.metamorphosis.org.mk – Фондација за одржливи информатички решенија*
- *www.kit.org.mk – Комисија за информатичка технологија на Р. Македонија*

АНЕКС: ИСО 17799 И 27001

БЕЗБЕДНОСТ НА ИНФОРМАЦИИТЕ И ЗОШТО ДА СЕ ШТИТИМЕ?

**МОТО на безбедност на информациите –
Доколку не сакаме самите себе да си помогнеме,
никој не може да ни помогне**

Информациите претставуваат крвоток на секоја организација

Што подразбираме под информација?
„ИНФОРМАЦИЈА е средство на организацијата, кое како и сите други деловни средства, има вредност за организацијата и поради тоа е потребно да биде соодветно заштитена"

Кои се основни типови информации?

- Испечатени или напишани на хартија
- Чувани во електронска верзија (компјутер, диск, цеде,..)
- Испратени преку пошта или други електронски врски
- Прикажана на организациските промотивни материјали
- Кажани во разговори (директно или преку телефон)

Безбедноста на информациите е битна за успехот на секоја организација и бара ефективно управување

Што претставува безбедноста на информациите?
ОБЕЗБЕДУВАЊЕ ДОВЕРЛИВОСТ, ИНТЕГРИТЕТ И ДОСТАПНОСТ НА ПИШАНИТЕ, ИЗРЕЧЕНИТЕ И КОМПЈУТЕРСКИТЕ ИНФОРМАЦИИ

- Безбедноста на информациите ја заштитува информацијата од низа закани, со цел да обезбеди континуитет на работењето, да минимизира потенцијална деловна штета, да ги максимизира деловните резултати и да ги оправда инвестициите во безбедноста на информациите.

- Секоја организација, односно институција развива СОПСТВЕН систем за безбедност на информации со сопствен сет барања од аспект на заштитни мерки и контроли, како и на нивото на доверливост, интегритет и достапност.

Што конкретно значи тоа?

- **Доверливост** - Обезбедување дека информациите се достапни само за оние што се овластени да имаат пристап до нив.
- **Интегритет** - Осигурување на точноста и комплетноста на информациите и на методите за нивна обработка.
- **Достапност** - Обезбедување дека овластените корисници ќе имаат пристап до конкретните информации секогаш кога им е потребно тоа.

Кои се најчести закани по безбедноста на информациите?

- Самите вработени
- Ниската свесност за безбедносните аспекти на информациите
- Експанзија на користење компјутери и компјутерски мрежи
- Интернет и електронска пошта (e-mail)
- Напад од „хакерите” и од „вирусите”
- Елементарни незгоди (пожар, поплава, замјотрес)
- Тероризам

ДЕНЕШНА ВИСТИНА: „ПОЕВТИНО Е НЕШТО ДА СЕ НАПРАВИ, ОТКОЛКУ ДА СЕ ЗАШТИТИ“

КАКО ДА СЕ ЗАШТИТИМЕ ОД ИНФОРМАЦИСКАТА НЕБЕЗБЕДНОСТ?

Дилеми :

- **Лично прашање:** Дали може да ни се случи најлошото? Колкава е предизвиканата штета и колку таа ќе нè чини? Колку сме подготвени да вложиме во „осигурување"?
- **Општествено прашање:** Чувствуваме ли обврска за безбедност на информациите со кои располагаме?

Наш одговор е : Воведување Систем за безбедност на информации според ИСО 17799 препораките

Кои се целите на воведување безбедност на информации?

- Зголемена доверба кај клиентите и кај партнерите
- Намалување на ризиците во работењето
- Безбедност на деловни информации преку безбедносни контроли и заштити
- Усогласеност со интернационалните и локалните регулативи

Како до безбедност на информациите?

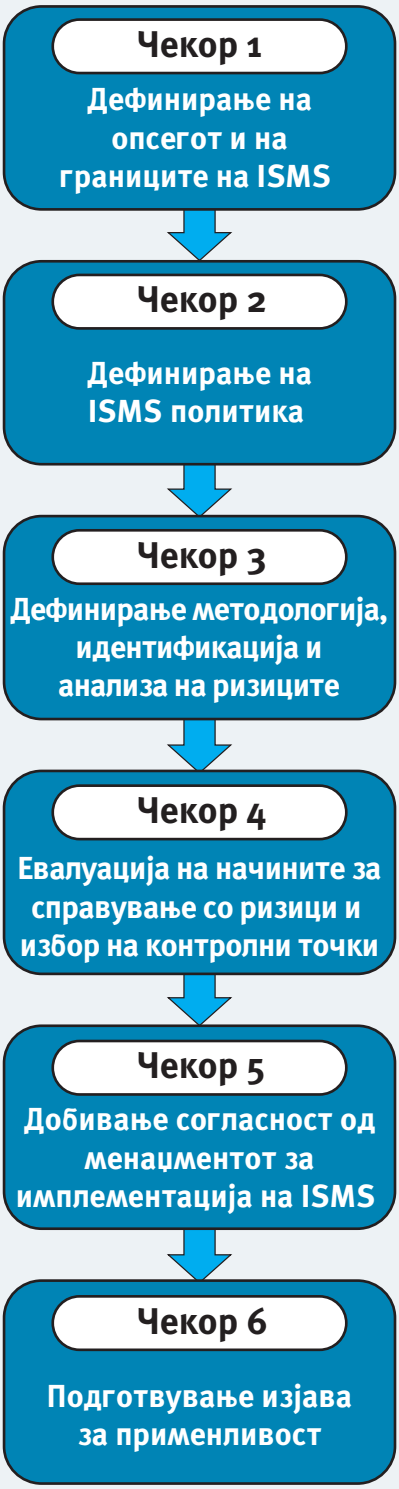
- **Со воведување** Систем за безбедност на информациите (Information Security Management System – *ISMS*) во согласност со ISO **17799** препораки за воведување Систем за безбедност на информациите
- **Со сертифицирање** според Стандардот за управување со безбедност на информациите ISO**27001**

Кои предуслови треба да се обезбедат?

- Свест за потреба од непрекинато работење, кое директно зависи од безбедноста на информациите
- Прифаќање на одговорноста за имплементација на ISMS од раководните структури
- Прифаќање на одговорноста за спроведување на ISMS од СИТЕ вработени
- Организиран пристап
- Посветеност и дисциплина во применувањето
- Подготвеност за перманентно подобрување
- Транспарентност на ISMS (информираност на вработените, клиентите, партнерите)

Како се воведува Систем за безбедност на информациите?

- Преку имплементирање соодветни заштитни мерки и контроли (политики, практики, процедури)
- Следејќи ги препораките од ISO 17799 - водичи за имплементација на систем за управување со безбедност на информациите базиран на индустриските најдобри практики.
- ISO 17799 има 11 контролни точки, кои опфаќаат повеќе безбедносни категории
- Воведувањето ISMS е комплексен процес презентиран во 6 (шест) чекори опишани во приложената шема



- Првите 2 чекора се клучни за успехот на имплементацијата на Системот за управување со безбедноста на информациите - ISMS. Тие опфаќаат дефинирање на опсегот, границите и политиката на системот. Дефинирањето се базира на основните карактеристики на организацијата, како што се големината, ресурсите, типовите на информации со кои располага, нормативата по која работи итн. За овие два чекора потребна е целосна поддршка и активен ангажман на менаџментот на организацијата.

- Третиот чекор го опфаќа оценувањето на ризиците за информциите на организацијата. Најпрво се дефинира пристапот и методологвијата за оцена, а потоа следи идентификација и анализа. Резултатите се листа на идентификувани ризици и извештај за влијанието на ризиците.
- Четвртиот чекор ги утврдува начините за справување со идентификуваните и анализираните ризици, определува контролни точки во согласност со стандардот и утврдува контроли што треба да се воведат.

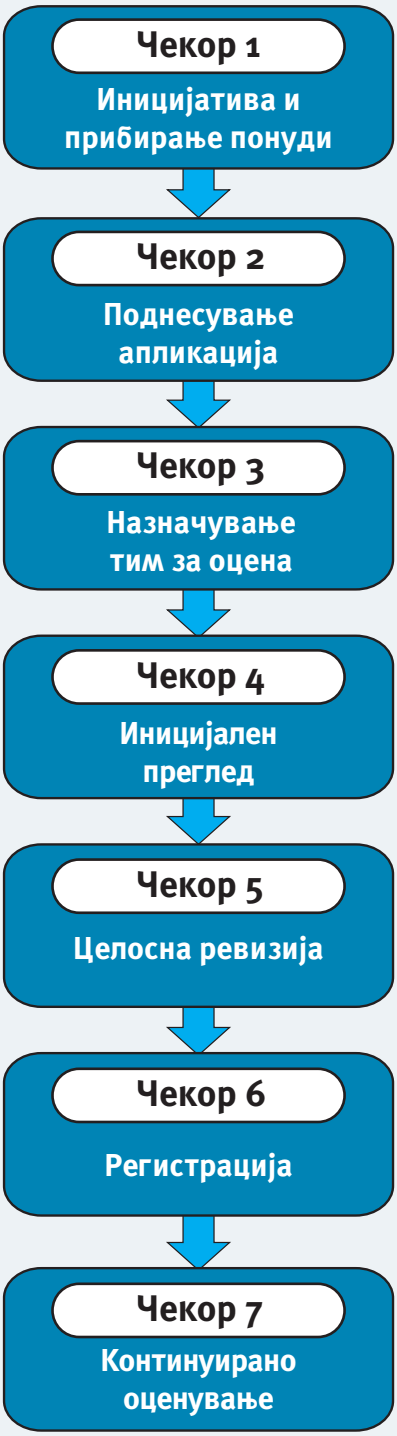
- Петтиот чекор го опфаќа добивањето на согласност од раководството за добиените резултати и имплементацијата на соодветни контроли.

- Последниот чекор (6) претставува документирање на избраните контролни точки и воведените контроли, како и причините за нивниот избор или правењето исклучоци.

КАКО ЗНАЕМЕ ДЕКА НАШИОТ СИСТЕМ Е БЕЗБЕДЕН?

Нашиот одговор е :
Сертификација на Системот за управување со безбедност на информациите, според ИСО 27001

Сертификацијата според ИСО 27001 се одвива во следните чекори:



Чекор 1: Покренување иницијатива за сертификација, анализа на опциите за сертифицирање и потенцијални сертификациски куќи и барање прелиминарни понуди за сертификација.

Чекор 2: Избор на сертификациска куќа и достава на формална апликација.

Чекор 3: Врз база на добиената апликација, сертификациската куќа определува ревизорски тим задолжен за сертификација и помош при развојот на вашиот ISMS систем.

Чекор 4: Првичен преглед на главните процеси и соодветната документација од страна на ревизорскиот тим.

Чекор 5: Спроведување целосна ревизија од страна на ревизорскиот тим, поднесување на извештај од ревизијата и препораки за подобрување.

Чекор 6: Како резултат на успешна ревизија, сертификациската куќа ви доделува сертификат на кој е јасно истакнат опсегот на вашиот Систем за управување со безбедност на информациите - ISMS.

Чекор 7: По успешната сертификација, ревизорскиот тим има обврска да ја посетува вашата организација редовно секоја година, со цел да го провери вашето работење и да ви помогне во процесот на подобрување.

Кои се придобивките од сертифициран Систем за управување на безбедност на информациите ?

- Врвниот менаџмент презема одговорност за безбедноста на информациите
- Независна потврда на Вашиот ISMS Систем и потврда дека се следат соодветните закони и регулативи
- Зголемена доверба кај Вашите партнери, заинтересирани страни и клиенти (Сертификацијата покажува ‘due diligence’)
- Ја подобрува Вашата конкурентност
- Поголема свесност за безбедност кај вработените
- Развиен механизам за мерење на успешноста на ISMS
- Редовните ревизии придонесуваат за континуирано подобрување во развојот и во напредокот на организацијата

СИСТЕМОТ ЗА УПРАВУВАЊЕ СО БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ ВИ ОБЕЗБЕДУВА ДА ГИ ЗАШТИТИТЕ ИНФОРМАЦИИТЕ КОИ СЕ БИТЕН РЕСУРС НА ВАШАТА ОРГАНИЗАЦИЈА.

ЦИП - Каталогизација во публикација
Национална и универзитетска библиотека
„Св. Климент Охридски“
Скопје

007:004.056

НАСОКИ за информациска сигурност / (автори на текстот Сашо Мицков ... др.). - Скопје : Фондација Метаморфозис, 2007. - 72 стр.; илустр. ; 30 цм

ISBN 978-9989-2792-0-1

1. Мицков, Сашо (автор)
а) Информациски системи - Безбедност
COBISS.MK-ID 70849546