

НОРМАТИВНИ АСПЕКТИ ЗАШТИТЕ ПОДАТАКА И ИНФОРМАЦИЈА

сци Драган Ж. Николић дипл.крим.

Апстракт: У раду се указује на значај података и информација. Информација је драгоцену робу коју није лако добити, употребити и што је још важније – сачувати. На свом путу од настанка до коришћења информација може бити нападана, модификована, изобличена, коришћена у разне сврхе, па и уништена. Због тога је веома важно на прави начин и одговарајућим средствима заштитити информацију у било ком облику. У раду су представљени нормативни аспекти њихове заштите односно организациони, кадровски и правни аспект заштите података и информација. Од њих би требало почети, максимално их искористити и са њима би требало покривати целу организацију и процес рада, независно од нивоа заштите који се захтева. Такво стање би требало доградити физичко - техничким и логичким мерама заштите у мери која ће обезбедити жељени ниво заштите.

Кључне речи: организација, кадрови, информација, податак, заштита.

Увод

Користити информацију значи руковати њеном грађом како би се постигао ефекат задовољења потребе за информацијом.¹ Уколико познавање ваших тајни може да повећа нечије богатство ви постајете објекат напада. Борба против злоупотреба информације не сме занемарити и мора јој се посветити посебна пажња.

Неоспорно је да постоји и друштвена и научна потреба да се сви проблеми који произилазе из злоупотребе података и информација истражују и успешно разрешавају. Човек је творац, носилац, корисник и узрочник отуђења, оштећења или уништења свих информација са једне стране док је са друге стране кључни чинилац безбедности. Он је креира, ствара и спроводи, он је и нарушава. Основни предуслов заштите података и информација је свест о потреби заштите. Тек када се догоди оно што је могло да се избегне долази до наглих промена у понашању и схватању.

Број претњи које могу угрозити објекте заштите практично неограничен, због чега их је и немогуће све предвидети. Разврставање у групе може да олакша анализу. Уважавајући и друге приступе, извршено је разврставање претњи – опасности у две групе, које пружају основ за целовито сагледавање проблема.

Најчешће изворе претњи можемо разврстати на:

- *Елементарне непогоде и природне катастрофе* (поплава, земљотрес, олуја, пожар): овај извор угрожавања је немогуће у потпуности предвидети. Неопходно и једино могуће је благовремено урадити реактивне процедуре које ће у случају наступања поменутих штетних догађаја, смањити настале штетне последице.

¹ Ињац-Малбаша В.: Наука о информацијама, Клио, Београд, 2005. стр.43.

- *Човек*, стим да можемо разврстати на ненамеран утицај: непажња, недисциплина, немар, незнање, лоша организација и намеран утицај: уништење, саботажа, диверзија, шпијунажа, ратно разарање, крађа, прислушкивање;

Угрожавање података и информација деловањем људи, без обзира да ли је оно учињено свесно или несвесно, у односу на средину одакле потичу можемо поделити на:²

- Унутрашњи извори угрожавања;
- Спољашњи извори угрожавања;
- Комбиновано.

Унутрашњи извори угрожавања представљају запослени радници. Угрожавање не може се прецизно сместити само у оквире радног времена већ и ван њега. Запослени ван радног времена, као последица недовољне безбедносне културе, свесно или несвесно могу угрозити пословање организације изношењем података од значаја. *Спољашњи извори угрожавања* подразумевају лица која нису у радном односу у институцији, а која својим штетним деловањем могу утицати на његову безбедност. *Комбиновани извори угрожавања* представљају заједничко штетно деловање лица која су запослена и лица која нису у радном односу.

Организација, односно руководство на унутрашњи извор угрожавања може највише утицати, управо из тог разлога предмет истраживања у овом раду је заштита података и информација исказана кроз три међусобно повезане логичке целине:

- Организациони аспект заштите;
- Кадровски аспект заштите;
- Правни аспект заштите.

Организациони аспект заштите

“Све организације су хијерархијски уређене. Људи на сваком нивоу подређени су онима изнад њих. Отуда, организација представља структурирану институцију. Уколико није структурирана, она само представља гомилу људи. Таква гомила не може ништа да створи; она само уништава ствари. Важно је створити организациону шему у којој ће се јасно видети задаци и одговорности појединаца”.

Theodor Levitt³

Добром организацијом обезбеђује се пуна ефикасност, економичност, продуктивност и квалитет, тако да се и са просечним кадровима могу остварити жељени резултати. Неадекватна организациона решења могу имати несагледиве нежељене последице на плану заштите. Примена адекватних организационих мера представља решење наведених и сличних проблема. Организационе мере усмерене су на избор најповољнијих организационих форми.

Кључна питања на која треба наћи адекватан одговор су:

- Утврђивање односа између појединца и групе;
- Права, обавезе и одговорност за свако радно место односно његовог извршиоца;
- Забране одређеног понашања и/или активности;

² Мандић Г.: Системи обезбеђења и заштите, Факултет цивилне одбране Универзитета у Београду, Београд, 2004, стр. 31-50.

³ Leavitt, H., Dill, W., Eyring, H., (1978) The organizational World, Harcourt Brace Jovanovich inc, New York.

- Утврђивање учесника и њихових активности;
- Опште и посебне мере заштите документације поверљиве природе;
- Утврђивање тренутног у односу на планирано стање.

Организациона структура представља формално утврђен систем односа између појединаца и група, у коме су њихове међусобне везе одређене распоредом задатака, одговорности и ауторитета.⁴ Формирање организационе структуре подразумева поделу рада, груписање и повезивање појединих врста послова, делегирање овлашћења и одговорности у обављању послова.⁵ Избор унутрашње организационе структуре зависи од конкретне ситуације, као што су број и структура извршилаца, расположива техника, врста и карактер података, број корисника и др., тако да су могући различити приступи.

Права запослени стичу заснивањем радног односа истовремено преузимајући одређене обавезе и одговорност за спровођење својих активности. Одговорност се може дефинисати као обавеза у односу на прописано и очекивано понашање, активност или резултат, односно обавеза да се задатак изврши законито, правилно, у разумном времену и у задовољавајућем обиму и квалитету.⁶ Осећај одговорности код кадрова је битан предуслов заштите. Неопходно је недвосмислено указати ко је за који део посла одговоран.

Рестрикције представљају спровођење одређених, немилих али неизбежних, поступака, као што су забрана пушења у одређеним просторијама, коришћење решова и грејалица у одређеним просторијама, забрана копирања одређених докумената, забрана приступа одређеним просторијама, примање приватних посета и сл.

Међутим, не потцењујући претходно, посебну пажњу свакако треба посветити регулисању уласка у и кретање по службеним просторијама. Неограничен приступ у све просторије није ни неопходан, ни пожељан, па кретање људи и материјала мора бити предмет посебне пажње. Све или одређене просторије треба означити као затворену зону. С тим у вези потребно је прописати режим уласка, кретања по и задржавање у таквој зони, а права везана за то свести на заиста реалне потребе.

У том смислу могуће је користити следеће врсте дозвола за улаз:⁷

- *Општа дозвола:* Приступ до свих просторија у свако време;
- *Ограничена дозвола:* Приступ до свих просторија у свако време, али само под надзором (нпр. чистачица);
- *Временска дозвола:* Приступ до свих просторија, али само у одређено време (нпр. ноћни чувар);
- *Просторна дозвола:* Приступ само до одређених просторија у било које време;
- *Просторно и временско ограничена дозвола:* Приступ само до одређених просторија и само у одређено време (нпр. кадрови за унос података или сервисери).

Право приступа рестриктивном простору, техници, подацима, информацијама и документацији треба дозволити и омогућити, по принципу "минимум овлашћења", само кадровима којима је то радно потребно и у мери адекватној тим

⁴ Петковић М.; Јанићијевић Н., Богићевић-Миликић Б.: Организација, ЦИД Економски факултет, Београд, 2006, стр.42.

⁵ Јовановић П.: Менаџмент, Графослог, Београд, 2004, стр.79.

⁶ Стајић Љ.; Мијалковић С.; Станаревић С.: Безбедносна култура, Драганић, Београд, стр. 64.; Стевановић О.: Руковођење у полицији, Полицијска академија, Београд, 2003, стр.117.

⁷ Петровић С.: Полицијска информатика, Криминалистичко-полицијска академија, Београд, 2007, стр.240-241.

потребама. Сваки радник би требало да познаје само оне елементе који су нужни за извршавање његових властитих задатака.

Стандард, технике, токове, активности и учеснике треба до детаља разрадити Нормативном регулативом радног процеса. Ефикасност на раду зависи не само од мотивације и способности радника, већ и од постојања одређених стандарда и дефинисаних процедура. Изградња и развој заштите мора се одвијати на планиран, организован и контролисан начин, тј. на основу усвојених конвенција и по одређеним правилима. Без овога, све је ван контроле и проблеми се само умножавају. Са становишта заштите, побољшање квалитета, једноставније и квалитетније спровођење контроле, указује на потребу увођења и примене адекватних процедура и стандарда.

Због свега тога неопходно је поставити формалне стандарде који управљају радом и процедурама, тј. дефинисати и донети Приручник стандарда који треба да обухвати следеће елементе: Архивирање података и информација; Обезбеђивање копија; Издавање, руковање и транспорт података и информација; Контрола података и информација; Припрема података и информација и сл.

Документација представља најчешћи извор откривања тајних података. Документи су сви писани, штампани, цртани или снимани материјали који садрже одређене податке. Злоупотреба документацијом може се спречити искључиво уколико су процедуре установљене, документоване, да се примењују и да се одржавају. Процедура је појединачни нормативни интерни акт којим се дефинише конкретно обављање и реализација одређеног посла и задатака.⁸ Са радним процедурама треба поступати као са званичним документима а измене треба да одобри руководство. Процедуре треба да наводе детаљна упутства за извршење сваког посла што обухвата:⁹

- Обраду и поступање са информацијама;
- Најраније време отпочињања посла и најкасније време завршетка посла;
- Упутства за поступање у случају ванредних догађаја;
- Контакт за подршку у случају неочекиваних тешкоћа у раду.

Контрола као функција представља активност праћења понашања организационих елемената и реализације постављених задатака. Контроле омогућују да се недозвољене активности могу правовремено открити, а могућност за извршавање криминалних радњи значајно редуцира. Контрола омогућује откривање слабости заштите и предузимање одговарајућих акција у циљу њиховог елиминисања.

Роберт Ј. Моклер (Robert J. Mockler)¹⁰ дефинише контролу као "системски" покушај да се поставе стандарди за учинак помоћу планираних циљева, да се пројектује систем информативне повратне спреге, да се упореде стварни резултати са унапред утврђеним стандардима, да се утврди да ли има одступања, да се измери њихов значај и да се предузму мере како би се сви системски ресурси користили на најефикаснији начин ради остварења циљева.

Из наведене дефиниције се види да контролу чине четири фазе:

- утврђивање стандарда и метода за мерење резултата,
- мерење резултата,

⁸ Милошевић М.: Физичко-техничко обезбеђење и противпожарна заштита, ИП Глосаријум, Београд, 2006, стр.18

⁹ ИСО 17799: Информационе технологије – правила праксе за управљање сигурношћу информација, Факултет безбедности Универзитет у Београду, Београд 2008, стр. 45-46.

¹⁰ Robert J. Mockler, The Management Control Process, Prentice Hall, Englewood Cliffs, N.Y., 1984, стр.2. Стевановић О.: Руковођење у полицији, Полицијска академија, Београд, 2004, стр.208.

- упоређивање резултата са стандардима и
- предузимање корективних акција (уколико је потребно).

Основна претпоставка квалитено спроведене заштите је могућност контроле. Уколико не постоји контрола заштита ће временом ослабити и неће служити својој сврси.

Контрола има троструку функцију:¹¹

- *Превентивну*, избегавање нежељених догађаја;
- *Дедуктивну*, откривање нежељених догађаја;
- *Корективну*, неутралисање негативних ефеката нежељеног догађаја.

Међутим, као што није пожељно запоставити контролу, тако је непожељно претеривати са њом. Претеривање спутава иницијативу и акције и изазива осећај неповерења, а као крајњи резултат јавља се несамосталност у раду потчињених.

Кадровски аспект заштите

Неопходно је имати у виду да је човек, с једне стране, носилац заштите података и информација док са друге стране представља потенцијалну опасност. Питање кадрова представља једно од кључних питања на плану заштите. Увођење кадрова омогућава да се организациона структура покрене, да се обављају планирани задаци и достижу планирани циљеви. Претња од "инсајдера"¹² у све већем је порасту. Под појмом "инсајдер" не можемо сматрати само стално запосленог радника институције, већ све оне који имају унутрашњи приступ систему.

Лица са унутрашњим приступом можемо сврсти у више категорија:¹³

- Стално запослено особље;
- Бивши радници;
- Запослени у кооперантским компанијама;

Запослено особље, поготово неопрезни и незадовољни радници, вероватно представљају највећу претњу. Имају свакодневни приступ осетљивим информацијама и за злоупотребу им је често потребан веома низак ниво образовања. Веома велики претњу представљају *бивши радници* компаније, било да се ради о отпуштеним радницима било да се ради о људима који су прешли из једне у другу компанију, поготово конкурентску. *Кооперантске компаније* могу представљати велики проблем за безбедносне системе јер често имају приступ осетљивим подацима.

У домену кадровске политике неопходно је применити све расположиве мере којима би се опасност од "инсајдера", ако не потпуно елиминисала, а оно бар свела у прихватљиве границе. Те мере се односе на:

- Планирање људских ресурса;
- Избор кадрова;
- Радну адаптацију;
- Безбедносно образовање и
- Стручно усавршавање;

¹¹ Петровић С.: Полицијска информатика, Криминалистичко-полицијска академија, Београд, 2007, стр.242.

¹² Инсајдер: од енгл. Речи "inside"(унутра) – неко изнутра, ко има приступ информацијама, добро упућен; запослени у институцији који има приступ осетљивим подацима.

¹³ Параушић М.: Инсајдери – највећа претња информационим системима, Безбедност 5/05, стр. 870.

а циљ им је да се оствари.¹⁴

- Заштита података и информација помоћу кадрова што подразумева да на кључна места буду постављени проверени, поуздани и стручни кадрови. Без обзира да ли су кадрови проверени или не, не може се узети за готово да су сви кадрови и поуздани.
- Заштита података и информација од кадрова подразумева, с обзиром да највећа опасност прети од човека, да сваки радник буде предмет перманентне пажње руководиоца. Посебну пажњу треба усмерити на индиције¹⁵ које бу указале на непоштење, склоност алкохолу, коцки и дроги, финансијске и породичне проблеме и сл.
- Заштита самих кадрова подразумева заштиту од сопствених ненамерних пропуста и грешака. Заштита кадрова спроводи се њиховим безбедносним образовањем и развијањем безбедносне културе као и стварањем таквог система рада и радних услова где ће грешке бити сведене на минимум.

Планирање људских ресурса је процес у којем се на основу антиципираних промена у интерном и екстерном окружењу предвиђају потребе за кадровима.¹⁶ Утврђивање потреба за кадровима представља типичну планску активност и почетну фазу у процесу кадрована. Потреба за кадровима се спроводи на основу стеченог искуства и раније праксе. Да би се одредио потребан број запослених и њихова квалификациона структура неопходно је анализирати послове и задатаке.

Анализу посла можемо дефинисати као систематски поступак утврђивања природе и садржаја посла (задатака, дужности и одговорности) услова и метода рада, као и психофизичких особина које посао захтева.¹⁷ Основни резултати процеса анализе посла су опис посла (радног места) и спецификација посла (радног места). *Опис посла* (радног места) је писани документ који описује које активности се обављају на конкретном радном месту. Овај опис такође садржи информације о опреми или инструментима које је потребно користити на одговарајућем радном месту, као и радне услове у којима се дати посао обавља. *Спецификација посла* (радног места) садржи потребна знања, вештине, способности и друге личне карактеристике неопходне за обављање конкретног посла.

Услове за пријем радника треба да дефинише руководство имајући у виду послове које новопримљени радник треба да извршава, као и могуће последице од нестручног, немарног или неодговорног обављања тих послова.

Избор кадрова представља једну од најсложенијих и најзначајнијих фаза у процесу кадрована. У овој фази треба извршити селекцију пријављених кандидата и изабрати најбоље, односно оне који најбоље одговарају траженим захтевима за одређена радна места.¹⁸ Основни критеријум код избора кадрова је њихова стручност за послове и задатке које би требали да обављају. Ову карактеристику је формално најлакше и проверити (дипломе, дужина радног стажа, садржај радног искуства и слично).

У организацијама у којима се захтева виши ниво заштите, односно у којима је значајно присутна безбедносна компонента радних места, стручност је само потребан, али никако и довољан услов. Оваквим организацијама требају комплетне

¹⁴ Петровић С.: Полицијска информатика, Криминалистичко-полицијска академија, Београд, 2007, стр. 259-260.

¹⁵ Индиција: у криминалистичкој терминологији индиције означавају утврђене чињенице или околности које посредно указују на кривично дело, односно на његовог учиниоца.

¹⁶ Петковић М.; Јанићијевић Н.; Миликић Б.: Организација, Центар за издавачку делатност Економског факултета у Београду, Београд, 2006, стр. 453.

¹⁷ Гузина М.: Кадровска психологија, Београдски издавачко-графички завод, Београд, 1980, стр. 147.

¹⁸ Јовановић П.: Менаџмент, Графослог – Београд, Београд, 2004, стр. 113-114.

личности, моралне, физички здраве и психолошки стабилне. Зато, код избора кадрова критеријуми би требало да буду знатно шири. Ту спада биографија и радна карактеристика без "мрља", као и лекарско уверење о адекватном здравственом стању.

За добијање "целовите слике" о кандидату погодно је користити технике интервјуа и анкете у циљу стицања знања о ставовима, осећањима, пороцима, плановима и жељама, као и прикладне врсте тестирања знања, способности и личности кандидата, уз, ако је могуће, учешће психолога и психијатра. Кључни елемент код избора кадрова је њихова квалификованост за послове које ће извршавати. Треба тежити избору кадрова чија је квалификованост оптимална у односу на захтеве радних места. Сваки несклад може веома неповољно деловати и на морал радника и на заштиту.¹⁹

Недовољно квалификован радник ће извршавати своје послове ван важећих стандарда, што резултира бројним грешкама. С друге стране недовољно квалификован радник негативно делују и на своје окружење, јер његове колеге постају незадовољне због чињенице да морају радити више. Радник чије квалификације значајно превазилазе захтеве радног места, перманентно ће тежити побољшању сопствене позиције извршавајући без већег напора изузетно своје задатке. Уколико његова тежња не резултира признањима и очекиваним напредовањем, последица може бити незадовољство усмерено на посао, околину, руководство или целу организацију.

Лица која су испунила предвиђене услове неопходно је да прођу и безбедносну проверу. Безбедносна провера особља пре свега обухвата процену да ли се за неког појединца у погледу лојалности, поверљивости, поузданости и веродостојности може дати овлашћење за приступ поверљивим подацима и информацијама, а да то не представља неприхватљив ризик за безбедност информација. Безбедносну проверу је потребно спроводити и за лица која су само привремено у контакту с поверљивим информацијама. Ове провере спровode се у опсегу који је прописан за доступан ниво поверљивости, као и уз знање и пристанак особе која се проверава. Лица која су прошла безбедносну проверу даје се понуда за посао и тек када је они прихвате процес селекције је завршен. Након пријема на радно место пре него се кандидат упуту у све детаље пословања треба обавити додатну проверу довођењем у искушење кандидата како би се проценила реакција и на ту ситуацију. Након свих провера и позитивних резултата кандидат се инкорпорира у пословни систем.

Адаптација људи у радној околини био је и остао значајан психолошки проблем. Тако, флукуација, изостанци, повреде, ефикасност људи на раду зависе у великој мери и од успешне адаптације на радну ситуацију. Радна адаптација је активно прилагођавање човека професионалним и социјално-психолошким захтевима, процес у коме се формирају нове навике, вештине, и знања, активно укључивање појединца у колектив и групу,²⁰ добијање и продубљивање постојећих знања, задовољство радом и радним местом.

Професионална адаптација се односи на процес стицања и мењања професионалних, стручних знања и вештина, формирање неких особина личности неопходних за успешно обављање датог посла. Овај вид адаптације се изражава и у развоју позитивног односа, става према изабраном занимању и врсти посла који појединац обавља. Флукуација, изостанци, несигурност, избегавање одговорности могу да представљају показатеље професионалне адаптације. Наведени облици

¹⁹ Петровић С.: оп. цит, стр. 246-248.

²⁰ Гузина М.: оп. цит, стр. 57-65.

понашања могу да буду последица неусклађености између индивидуе и радне улоге, захтева који се пред њега постављају, односно, како их он сам опажа и доживљава.

Социо-психолошка адаптација се односи на улазак и постепено уклапање појединца у нову социјалну средину, групу и радну организацију, тј., на процес у коме појединац постепено постаје члан колектива. Социо-психолошка адаптација се дефинише као сложен процес који обухвата когнитивне, емоционалне и бихејвиоралне компоненте.

Когнитивна компонента се односи на процес комуникације, општења с радним људима у групи и колективу, упознавање групних односа, норми, упознавање популарности појединих радника, руководиоца, односа између група итд. Овде је могуће правити разлику између упознавања и укључивања у формалну, а потом и у неформалну структуру. Емоционална компонента се огледа у формирању позитивних ставова, задовољству постојећим интерперсоналним односима и симпатијама према људима у групи и радној организацији. Бихејвиорална компонента – се односи на активну укљученост и допринос појединца социјалном животу групе и колектива. Крајња фаза и домет овог активног укључивања појединца у социјалне односе, представља идентификацију индивидуе с групом и колективом.

Код распоређивања новопримљених кадрова препоручује се крајња опрезност и одређена поступност код њиховог увођења у посао, које би требало да се одвијају по принципу: од једноставних ка сложенијим, од мање важних ка значајнијим пословима. Кандидата детаљно треба упознати са организационом шемом, садржајем рада, позицијом свог радног места у хијерархији, са надређеним и подређеним радним местима, дужностима и правима, као и са важећим мерама, процедурама и правилима заштите.²¹ Препоручује се да се новопримљени радник у старту повеже са оним радницима који су по природи комуникативни, веселе природе, спремни да сарађују и, посебно, да помогну. Овакав приступ може значајно да допринесе његовом бржем прилагођавању и ефикаснијем укључивању у радни процес и да са психолошког становишта утиче на формирање његовог позитивног односа према новој радној средини и обавезама у њој.

Безбедносно образовање треба да пружи довољно знања о потребама, разлозима и начинима заштите, да објасни потребе и разлоге поштовања и придржавања стандардних мера и процедура заштите, да развија "безбедоносну културу" и да подсећа на обавезе у односу на заштиту.²² Елементарне основе заштите података и информација (безбедносни термини, концепти, осетљивости, претње, последице) стичу се подизањем свести о потреби заштите, а надоградња се реализује кроз обуку. Сврха свести презентира се једноставно са фокусирањем пажње на заштиту што омогућује појединцима да препознају и разумеју потенцијалне ризике и сходно томе и важност заштите. Свест креира осетљивост запослених на претње и спознају да треба штитити податке и информације. Подизање свести запослених о важности чувања података и информација мора бити свакодневна брига. Релативно честом неофицијелном комуникацијом или путем семинара запосленима се предочава какве штете могу настати губитком одређених информација и како се то може на њих саме одразити. Једна од превентивних мера би могла бити и периодично одржавање информативних састанака о заштити. Разматране теме би требале да освеже и иновирају раније стечена знања, али и да подсети на обавезу у односу на заштиту, посебно што временом слаби свест о

²¹ Петровић С.: оп. цит, стр. 248.

²² Петровић С; Ћирић В.: оп. цит, стр. 18.

значају заштите и смањује се опрезност и будност према недозвољеним активностима.

Стручно усавршавање представља напор да се побољшају перформансе запослених на њиховом радном месту. Усавршавање подразумева надоградњу специфичних знања, способности, вештина, ставова или понашања.²³ Организованим стручним усавршавањем може се отклонити опасност која прети од нестручних, неспособних и неодговорних кадрова. Најопштије речено, ефикасност на раду зависи не само од мотивације и способности радника, већ и од његове стручности, познавања посла и одговарајућих радних навика и вештина. Недовољна, или неодговарајућа знања, објективно излажу појединца тешкоћама и незадовољству у раду.

Правни аспект заштите података

Проблем заштите података и информација превазилази реалне могућности њиховог успешног и целовитог разрешавања организационим и кадровским аспектима па тежиште тог разрешавања треба померати и ка другим областима, а пре свега правној, чији би механизми требало да повећају вероватноћу жељеног понашања. Огромна количина података и информација најчешће није у довољној мери и на адекватан начин заштићена. Један од основних узрока оваквом стању је непостојање јединствених основа за разрешавање овог изузетно сложеног и , са друштвеног аспекта, веома значајног проблема.

Законска регулатива заштите би требала да обухвати:²⁴

- Дефинисање циља заштите;
- Разрађене критеријуме за класификацију;
- Основне облике заштите;
- Дефинисање нивоа одговорности;
- Обавезу пријављивања свих облика злоупотребе;
- Мере друштвене контроле;
- Казнене одредбе.

Дефинисање **циља заштите** односи се на обезбеђење и заштиту интегритета, расположивости и тајности података и информација.

Класификација података и информација би се морала извршити по степену значајности, као и према степену поверљивости.

Основни **облици заштите** би обухватали:

- Начин обезбеђења веродостојности података;
- Мере и поступке за спречавање неправилног, злонамерног или неовлашћеног мењања, отуђивања, оштећења, уништавања, објављивања или коришћење података и информација;
- Условне и критеријуме за рад са поверљивим подацима.

Ниво одговорности подразумева потребу да за податке и информације од значаја треба пописати и именовати њеног власника. Пописивање података и информација помаже да се осигура одржавање одговарајуће заштите.

Пријављивање злоупотребе је обавеза свих. Сва лица обавезна су да пријаве руководиоцу органа у којем су запослени или органу унутрашњих послова

²³ Петковић М.; Јанићијевић Н.; Миликић Б.: оп. цит, стр. 464-467.

²⁴ Петровић С.: Полицијска Информатика, Криминалистичко-полицијска академија, Београд, 2007, стр.203.

неовлашћен приступ тајним подацима и да дају изјаву о околностима под којима су стекла увид у тајне податке.

Мере друштвене контроле подразумевају праћење остваривања и спровођења законске регулативе. Када су захтеви за сигурност дефинисани, треба одабрати и уградити контроле како би се осигурало да ће ризици бити смањени на прихватљив ниво. Избор контрола треба да се заснива на трошковима уградње у складу са ризицима који се умањују и могућим губицима уколико дође до губитака одређених података и информација. У обзир треба узети и чиниоце који немају новчани карактер као што је губитак угледа.

Казненим одредбама свако угрожавање или покушај угрожавања података и информација мора бити предвиђено а носиоци угрожавања морају сносити одређене санкције.

Р. Србија још увек нема Закон о класификацији информација, који би требало да обезбеди систематску правну контролу тајних података по угледу на земље Европске уније. Та област је код нас регулисана парцијално или кроз појединачне одредбе, због чега је рад државних органа, а нарочито специфичних институција у области безбедности, још нетранспарентан. Још увек на снази стандарди из шездесетих година, те се тајне разврставају на: Државне; службене и војне, са степеном тајности: строго поверљиво, поверљиво и интерно, што није у складу са законодавством у ЕУ. Земље чланице ЕУ не познају посебне врсте тајни, већ само четири степена тајности података – државна тајна, строго поверљива тајна, поверљива тајна и интерна тајна.

У тој области влада "потпуни хаос", јер је поступање са тајним подацима сада регулисано са више од 400 закона и подзаконских аката, парцијално или кроз појединачне одредбе. Због непостојања закона може се лако манипулисати тајним информацијама. С обзиром на то да ова област законски није регулисана, сваки податак може да буде државна или службена тајна, ако се тако одлучи или ако то некоме одговара.

Правни систем морао би да на адекватан начин уреди чување, обраду, приступ и контролу поверљивих информација. Требало би усвојити Закон о класификацији тајности информација. На тај начин би се остварио механизам контроле који искључује да се тајном избегне одговорност, уколико не постоје јасни критеријуми шта се сме прогласити тајном имамо низ злоупотреба. Поступање са тајним подацима је унификована скоро у целом свету и подразумева јасно дефинисање неких важних питања - да ли постоји орган власти који има увид у све тајне податке, ко може да се бави класификацијом података и ко да их користи, однос између органа власти по питању размене информација, као и да ли треба да постоји централни орган који би се бавио приступом информацијама.

Огромна количина података односи се на податке о личности. Приватност је једно од основних људских права која су везана за личност човека, којима се обезбеђује интегритет и дигнитет људској личности и која захтевају очување тајности и слободе приватног живота. Приватност подразумева право појединаца да сами одреде обим личних информација које желе да деле са другима. Она укључује њихово право да контролишу прикупљање, меморисање и дисеминацију њихових података или информација о њима самим.²⁵

Доласком до личних података злонамерна лица могу њиховом манипулацијом утицати на наш друштвени и професионални статус. Друштво мора, у законским оквирима, да обезбеди сваком грађанину право на приватност као и заштиту свих

²⁵ Петровић С.: оп. цит., стр. 205.; Дракулић М.: Основи компјутерског права, Друштво операционих истраживача Југославије, Београд, 1996, стр. 65.

података које лице услужно даје одређеним организацијама. Грађани који податке о себи и својима уступају на коришћење друштву морају имати поверење у то друштво, да оно што је добијено од грађана неће бити злоупотребљено. Држава мора законима да уреди прикупљање информација, њихову обраду, чување, коришћење и заштиту тајности података.

Значајно је да доношење законских прописа, који се односе на заштиту података и информација, буде у складу са међународним стандардима и смерницама, уважавајући туђа искуства и сопствене специфичности. С обзиром на потенцијалне могућности ових дела, санкције би морале бити веома строге – од високе новчане казне и вишегодишње казне затвора до забране вршења делатности које се односе на заштиту података или које имају додирних тачака. На овај начин санкције би, поред кажњавања учинилаца ових кривичних дела, служиле и као снажно превентивно средство за застрашивање и одвраћање потенцијалних учинилаца.

Закључак

Човеку су одувек биле потребне информације. Проста људска радозналост, жеља за знањем, стратешки интереси, прикупљање, обрада и употреба информација, све то постоји у људским друштвима од самог почетка и у тежишту је процеса развоја. Нема безопасних података. Сваки, па и најбезазленији податак, може да представља потенцијалну опасност за физичка и/или правна лица, одређену друштвену, породичну заједницу и/или неку другу скупину. Обезбеђење сигурности података једно је од најзначајнијих и најделикатнијих питања са којима се срећу сва друштва. Све већа потреба за подацима и све већи страх од њихове злоупотребе довели су до неопходности њиховог посебног третмана.

У Р. Србији се, за разлику од других земаља у транзицији, отицање важних сазнања и информација још увек не сматра никаквом штетом. Код нас не постоје стручњаци који би се супротставили делујући најпре превентивно, а потом и оперативно. То су веома уске специјалности и посебна знања којима се код нас бави мали број људи, а ни друштво се, нажалост, не труди много да их обучи и ангажује.

Уколико се пројектовању заштите не поклони дужна пажња од самог почетка развоја па кроз сваки следећи корак до коначне инсталације, сигурност података ће у великој мери бити угрожена. Реално, нико не може да нам гарантује стопроцентну заштиту. Јер ма колико ми неки систем технички направимо савршеним, њега ипак користе људи. Људски фактор је и даље једно од кључних места где безбедност пуца. Наравно, код озбиљнијих система, где је вредност података који се штите велика, висок је и ниво "безбедносне културе" особља, тако да су напади ове врсте тамо мало вероватни.

Да би се систем заштите изградио потребно је створити одговарајући кадар, а затим га оптимално распоредити. Мора да се разради прецизни правилник за *заштиту података на аудио и визуелна средства* (рачунари, радио уређаји, факс уређаји, мобилни телефони, фиксни телефони итд), и *заштити свих врста писаних докумената* (штампачи, апарати за копирање и сл.).

Информације треба класификовати како би се указало на потребе, приоритете и степен заштите. Информације имају променљиви степен осетљивости и критичности. Неки елементи могу захтевати додатни степен заштите или посебан поступак. Систем за класификовање информација треба примењивати како би се дефинисао одговарајући скуп нивоа заштите и исказала потреба за посебним мерама у поступању.

Проблем заштите података и информација је занемарен. Узроке оваквог стања можемо наћи у непостојању законске регулативе која директно регулише ову област. Надамо се да ће примена законских решења у великој мери сузбити и предупредити бројна противправна поступања у односу на тајне податке и информације чиме ће заштита података и информација добити квалитетно виши ниво. Будући да је наша стварност последњих година забележила бројне случајеве злоупотребе крајње је време да се држава не само превентивним мерама већ и системом кривичних санкција ухвати у коштац са оваквим неодговорним појединцима и групама.

Неопходно је предузети низ друштвених, правних, техничких, организационих и других мера, као и примену разних метода како би се обезбедила њихова сигурност. Да би примена мера и метода била ефикасна, мора бити синхронизована и међусобно тако повезана да ни једна карика у ланцу не изостане. Безбедност информација је веома важна компонента укупне безбедности, па се њеној анализи и проучавању мора придавати одговарајућа пажња. Питањима безбедности информација мора се водити рачуна у свим областима друштвеног живота. Неадекватно третирање питања безбедности информација може довести последица у свим сферама друштвеног живота у лепези од тривијалних до катастрофалних.

Литература

- [1.] A Users' Guide: How to Raise Information Security Awareness, June 2006, <http://www.iwar.org.uk/comsec/resources/ENISA/infosec-awareness.pdf>
- [2.] Гузина М.: Кадровска психологија, Београдски издавачко-графички завод Београд, 1980.
- [3.] Даничић М., Стајић Љ.: Приватна безбједност, Висока школа унутрашњих послова, Бања Лука, 2008.
- [4.] Друштвена самозаштита: Правилник о државној и службеној тајни и њиховој заштити, Београд, 1981.
- [5.] From wikipedia, the free encyclopedia: Information sensitivity, http://en.wikipedia.org/wiki/Talk:information_sensitivity.
- [6.] Ђорђевић И.: Заштита информација у ери информатизације људских активности, Факултет цивилне одбране Универзитета у Београду, Београд, 2007.
- [7.] ISO 17799: Правила праксе за управљање сигурношћу информација, Факултет безбедности Универзитет у Београду, Београд, 2008.
- [8.] Information Security: Raising Awareness, Version 1.0, 14 April, 2000, Treasury Board of Canada Secretariat, <http://www.cio-dpi.gc.ca/>.
- [9.] Јовановић П.: Менаџмент, Графослог, Београд, 2004.
- [10.] Комуџић М., Бучар Б.: часопис Модерна организација, Безбедност, 1970.
- [11.] Кулић Ж.: Управљање људским ресурсима у области безбедности и здравља на раду, Београд, 2007.
- [12.] Кукрика М: Управљање сигурношћу информација, INFO home, Београд, 2002.
- [13.] Лукић Р., Кошутић Б.: Увод у право, Научна књига, Београд, 1997.
- [14.] Leavitt H., Dill W., Eyring H. The organizational World, New York.
- [15.] Матић Г.: Основи физичко - техничког обезбеђења, Привредна комора Србије, Београд, 2006.
- [16.] Мандић Г.: Системи обезбеђења и заштите, Факултет цивилне одбране Универзитета у Београду, Београд, 2004.

- [17.] Милошевић М.: Физичко - техничко обезбеђење и противпожарна заштита, Београд, ИП Глосаријум, 2006.
- [18.] Милошевић М.: Систем државне безбедности, Полицијска академија, Београд, 2001.
- [19.] Milenović M.: Informacije – imovina zlata vredna“ (www.dataprotection2003.info);
- [20.] Параушић М.: Инсајдери - највећа претња информационим системима, Безбедност 5/05, Београд, 2005.
- [21.] Петровић С.: Полицијска информатика, Криминалистичко-полицијска академија, Београд, 2003.
- [22.] Петровић С.: Компјутерски криминал, Војноиздавачки завод, Београд, 2004.
- [23.] Петровић С.: Полицијска информатика, Криминалистичко-полицијска академија, Београд, 2007.
- [24.] Петровић С.: Безбедносна свест, обука и едукација - критичне компоненте заштите кибер - простора, Саветовање злоупотребе информационих технологија (ЗИТЕХ), Београд, 2006.
- [25.] Петковић М., Јанићијевић Н., Богићевић - Миликић Б.: Организација, ЦИД Економски факултет, Београд, 2006.
- [26.] Robert J. Mockler: The Managagement Control Process, New York, 1984.
- [27.] Родих Б., Ђорђевић Г.: Да ли сте сигурни да сте безбедни, Продуктивност, Београд, 2004.
- [28.] Council of Europe: The European Convetion on Human Rights, <http://www.hri.org/docs/ECHR50.html>.
- [29.] Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, http://www.art.pl/~fajgie1/Odo/En/conv_en.html.
- [30.] Стајић Љ.: Основи безбедности, Факултет цивилне одбране, Београд, 2005.
- [31.] Стевановић О.: Руковођење у полицији, Полицијска академија, Београд, 2003.
- [32.] Стајић Љ., Мијалковић С., Станаревић С.: Безбедносна култура, Драганић, Београд, 2005.
- [33.] Ињац-Малбаша В.: Наука о информацијама, Клио, Београд, 2005.
- [34.] Цигурски О.: Информатика, Факултет цивилне одбране Универзитета у Београду, Београд, 2002.

Normative aspects of data and information protection

Nikolić Ž. Dragan graduate criminalist, degree in specialized studies

Abstract: The work points out the importance and measures of protection of integrity, confidentiality and availability of data and informations. Therewith particularly are emphasized the inner sources of threats. Information is a precious commodity that is not easy to get and more importantly – to save. On its way from the beginning to the usage, the information may be attacked, modified, distorted, used for different purposes, and also,

destroyed. It is therefore very important to properly and with appropriate means protect information in any form. In the work are presented the normative aspects of protection, that is, organizational, personnel and legal aspects of data and informations protection. It should be started from them and use them at most, independently of the level of protection required. This situation should be upgrade with physical - technical and logical security measures in proportion that will provide the desired level of protection.

Keywords: organization, personnel, information, data, protection.