ЧОВЕШКИ ФАКТОР И ИНФОРМАЦИОННА СИГУРНОСТ

Христо ДОМОЗЕТОВ

Значителна част от човешката и социалната дейности като комуникациите, банковите услуги, резервациите за развлечения, пътувания и пр. се осъществява с помощта на информационните технологии. Основният въпрос, който възниква, е доколко могат да се повлияят хората, които работят с информационни технологии, така че да възприемат промените в организационните правила и навиците си, за да се осигури информационна безопасност, необходима за работата и живота?

С нарастването на обхвата и усъвършенстването на информационните системи съхраняваната информация не само се увеличава като обем и се променя в качествено отношение, но и се превръща в изключително важен и ценен обект за гражданите и обществото. Както посочва Н. Генов, "Чести са случаите, когато реализирането на определена идея за организационно рационализиране води със себе си формирането на нови образци от рационални процедури на дейност, т.е. на социални технологии."[1] Така че появата на обхватни информационни структури налага използването на съответните социални технологии - една от които е опазването на информацията. То е от жизнено значение както за правилното и успешно функциониране на администрацията, на въоръжените сили и на силите на реда и сигурността, така и за защитата на информацията за личността, за собствеността и правата на гражданите.

В съдържателен и задълбочен доклад по проблемите на международните измами експертът на Европейската комисия Вафа Моайед[2] посочва, че при различните видове измами в банковата сфера, в обществения сектор, при предварителните разплащания, при инвестиционните измами, фалшиви застраховки и пране на пари особена роля играят информационните технологии.

Независимо дали човек става жертва вследствие на алчността си, на наивността си или на липсата на познания за измамниците, на слабия финансов контрол или на стремежа да рискува при всякакви условия, той най-често попада в полезрението и действията на лица, използващи всички предимства на съвременните информационни и комуникационни средства. Престъпниците - без значение дали са представители на организираната престъпност, корумпирани служители и мениджъри или членове на малки престъпни шайки - са прекрасно информирани, мобилни са и благодарение на най-новите технически постижения могат да осъществяват трудно уловими финансови удари. Така например е известен случай, при който фалшив банкомат, който не дава нищо на клиентите, е монтиран до истински на една лондонска улица, за да събира информация за истински кредитни карти. Благодарение на нея в Испания се изготвят фалшиви кредитни карти, а парите са теглени на територията на Италия.

В резултат на подобна престъпна дейност жертвите - отделни индивиди или компании - губят пари или имущество; пропускат ползи; правят разходи за издирване и защита; за възстановяване на средства чрез съдебни дела, адвокати и пр.; губят репутацията си, клиентите и тяхното доверие. Държавните органи изразходват средства за създаване на организации за борба с подобни престъпления, за съдилища и затвори, но понасят загуби и от неизплатените данъци. Загуби за обществото произтичат от формиране на нечестна конкуренция (която, след като не плаща данъци, може да направи дъмпинг), загуби на инвестиции, намаляване на клиенти и по-ниска ефективност на производството, безработица в компанията, която е изиграна. Естествено тези, които са загубили, вдигат цените, за да компенсират. Твърди се, че в резултат само преките загуби от подобни международни измами за Европейския съюз са около 60 милиарда екю годишно.

Най-съществените пречки при разследване на подобни престъпления, свързани със съвременните информационни технологии, са разликите в подготовката и организацията на човешкия фактор, осигуряващ информационната сигурност, и различията в законодателствата на отделните страни. От значение е и фактът, че тези проблеми не навсякъде имат висок приоритет, както и разликата в наличните ресурси и опит в съответните административни и наказателни органи. Съществено за нашата проблематика е, че според редица изследвания в по-голямата част (повече от 80 %) от случаите на подобни компютърни престъпления достъп до търговските тайни или софтуерните кодове са имали служители от пострадалите фирми.[3]

Гореизложените факти, както и ширещата се практика да се подценява участието на човека в глобалните информационни процеси за сметка на

непрекъснатото усъвършенстване на технологиите, обуславят необходимостта от задълбочено разглеждане на проблемите на човешкия фактор при осъществяване на информационна сигурност.

Преди всичко обаче е необходимо да се направи уточнение на термини, които намират най-масово приложение в теорията и практиката на разглеждания кръг от проблеми.

Понятието *информационна сигурност* се използва от преди повече от 15 години, като в определението, дадено в Акта за защита на данните, приет във Великобритания през 1984 г., се отбелязва защитата срещу непозволен достъп, преобразуване, унищожаване или отказ на достъп до съхраняваните данни в информационните системи.[4]

Според нас "информационна сигурност" представлява защитата на автоматизирано обработвана информация срещу:

- Неправомерен достъп,
- Случайни или нарочни видоизменения,
- Случайно или нарочно унищожаване,
- Случайно или нарочно разкриване на съдържанието й.
- Излъчвания, издаващи нейното смислово съдържание.[5]

Както може да се установи, в допълнението към общоприетото определение е добавен още един вид защита и се отбелязва разликата в мотивацията на нарушителите (случайно или нарочно действие).

В една от последните си книги Шаламанов и Тагарев наред с част от горепосочените заплахи посочват и "разрушаване на информационната инфраструктура."[6] Както в тяхната, така и в наши и други публикации се изтъква, че *е необходимо* информационната сигурност да се разглежда не само и не толкова в тесен мащаб (например в рамките на дадена служба или фирма), а и като една от съставките на националната сигурност.

Информационната система включва:

- Всички категории от автоматизирано обработвана информация, включително програмите;
- Информационно-технологични устройства и съоръжения, включително компютрите, които принадлежат на дадена служба или се контролират от нея;
- Възприетите нормативи и правила, начините за реализиране на правата и контролиране на задълженията, необходими за функциониране на системата;
- Хората, които работят с компютърната техника и програмните продукти в системата, както и техните ръководители.

В случая проявяваме интерес преди всичко към последната по ред на изброяване, но в никакъв случай и по значение съставка.

Когато разглеждаме проблемите на *човешкия фактор,* ще използваме дефиницията на Гришченко, според който "човешкият фактор е обобщено понятие за човешка дейност. Активирането на човешкия фактор по същество означава активиране на производствената, социалната и… дейност."[7] Тук съществената разлика от разглеждането на проблемите на човека въобще е, че се подчертава неговата активна, очевидно съзнателна дейност, а не пасивното, съзерцателно състояние.

Същевременно при разглеждане на проблемите в информационната сфера е подходящо да се изтъкне, че човекът, субектът е производител, носител, разпространител, но и пазител на информация.[8]

Осъществяването на информационната сигурност предполага преди всичко формиране на политика на информационна сигурност - било на равнището на фирма или компания, на регионална или национална институция, или на национално (в бъдеще на планетарно) равнище.

ЗА ПОЛИТИКАТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Основните цели на политиката на информационна сигурност са:

- посредством подготовка на специалисти, осигуряване на техника и утвърждаване на нормативи да гарантира защита срещу злоупотреба със или загуба на информация;
- да утвърждава отговорностите и отчетността на ръководители и служители за информационните ресурси;
- да утвърждава изискванията за поверителност на информацията и начините за контрол на различните видове персонал;
- да утвърждава принципа на самооценка на служителите при навлизането и участието им в процеса на осъществяване на мерките за безопасност, както и в програмата за обучение и оповестяване на служителите за мерките за сигурност;
- да предотвратява нарушаването на управленските функции на ръководния състав в случай на загуба или злоупотреба с информация.

Подценяването на съвременните възможности на политиката на информационна сигурност в някои наши ведомства се дължи предимно на човешкия фактор. При наличието на сравнително ниска и несистемна компютърна грамотност на "масовия служител" у някои наши експерти, поели ръководството на компютърни или аналогични служби, се е формирало

неоправдано високо самомнение, водещо до принизяване на мерките за сигурност. Тяхното безгрижие се подхранва и от факта, че до този момент не са изградени национални и регионални компютърни мрежи, чрез които достъпът до данните да е улеснен и те да бъдат сериозно застрашени. Това обаче предстои в обозримо бъдеще.

При разглеждането на проблемите на информационната сигурност могат да се приложат най-малко два подхода. Група български научни работници с трайни интереси и опит в защитата на информацията, която публикува под псевдоним, анализира преди всичко мерките и средствата за защита в различни аспекти. Такива са например "юридически норми и социално обкръжение; административни и организационни мерки; физически средства за защита; средства за безопасност и достоверност, вградени в системата за обработката на данните."[9] Очевидно високият професионализъм на авторите от тази група обаче (доколкото може да се съди от немногобройните публикации) вероятно е бил насочен не толкова към разработване на цялостна система за информационна сигурност, колкото към решаване на някои твърде важни, но специфични и ограничени по обхват задачи. Не става ясно например за кое "социално обкръжение" става дума - за малката група професионалисти, за техните колеги от останалите служби в организацията или институцията, или за цялостната макросреда, която също влияе върху микросредата.

Според нас проблемите на информационната сигурност може да се изследват и разработват цялостно, без да се пренебрегва който й да е от аспектите. При това вниманието се съсредоточава върху участието на човешкия фактор в защитата на различните видове обекти - на информацията, на физическите обекти, в които се помещава компютърната техника, на самата компютърна техника, на програмните продукти, на комуникационните мрежи, на (и от) персонала, който работи с компютърната и комуникационната техника.

Без да се претендира за изчерпателност, може да се подчертае, че към основните компоненти на програмите за национална и локална информационна сигурност се отнасят[10]:

- Отговорностите на човешкия фактор за информационната сигурност;
- Преценка на риска;
- Безопасност, отнасяща се до персонала;
- Безопасност на физическите обекти;
- Безопасност за информацията;
- Безопасност за комуникационните мрежи;
- Безопасност за микрокомпютърната техника.

Научната обективност ни задължава да отбележим, че препоръките за практиката при осъществяването на информационната сигурност не могат да се създадат с усилията само на един изследовател или експерт или даже на нарочно създаден екип. Те са резултат от опита на много специалисти от различни страни за продължителен период от време. Така че споделените по-долу изводи и препоръки за практиката при някои от компонентите на информационната сигурност представляват синтезирани от нас обобщения от разговорите с експерти, от отговорите в интервюта и от рядко срещаните фрагментарни публикации. Естествено е да се очаква с усъвършенстването на техниката, технологиите и натрупването на специализиран опит тези препоръки да бъдат развивани и обогатявани.

ОТГОВОРНОСТИ НА ЧОВЕШКИЯ ФАКТОР

Както отбелязват австралийските учени Робърт Крос и Тони Уотсън, компютърната безопасност е една пренебрегвана област дотогава, докато редица обстоятелства не привлекат вниманието на ръководството върху потенциалните или реалните опасности - за съжаление след като инцидентът вече е налице.[11] Именно тогава започват и дискусиите относно това кой е отговорен за пропуска и кой не си е изпълнил задълженията. Всъщност често пъти подобни задължения не са били дори отбелязани в определен документ.

При създаването на служби за информационна сигурност висшето ръководство има три съществени функции: да насърчава хората, да улеснява разработката и внедряването на необходимите мерки и да контролира процесите. При разработване и въвеждане на програма за информационна сигурност тези функции са конкретизирани за различните етапи.

Човешкият фактор и управлението на информационната сигурност

Управлението на информационната сигурност изисква хората, които го осъществяват, да притежават съчетание от технически, административни способности и усет към маркетинга. Ръководството - независимо дали е отделен служител или голяма група ръководители или командири - би трябвало да полага усилия както за насочване на технически решения за решаване на проблеми на информационната сигурност, така и за овладяване на нарастващите информационни потоци на всички равнища на организацията.

При това е необходимо да се има предвид, че в последните години у нас при хората, ангажирани в работа с компютърна техника, се наблюдават характерни особености. Продължава да се откроява, както и в предходните периоди, недостатъчна или едностранчива квалификация за работа с компютрите. Формалният подход при обучението и банализирането на заплахите за

сигурността водят до нехайно отношение към спазването на мерките за сигурност, за защита на информацията. Честата смяна на указанията, в много случаи обусловена от спорадичната смяна на ръководители на различни равнища, преобразува нагласата за съдействие у служителите в нагласа към бездействие и изчакване, докато се случат неприятни събития. Несистемният контрол при неизяснени отговорности пораждат у служителите безразличие към информационната сигурност и насърчават имитационните, показни (за пред началството) действия.

За подпомагане на дейността на ръководството е целесъобразно създаването на многофункционалното звено за информационна сигурност. Основните отговорности на експертите в него включват:

- Разработване на политика, процедури и правила за сигурността, които да съвпадат с политиката на организацията и с общоприетите принципи за контрол при компютърната обработка на данни;
- Въвеждане на програма за сигурност, която включва класификация на информацията (степен на поверителност и др.), преценка на защитеността на охраняваните обекти и на евентуално застрашаващи ги събития;
- Разработване и провеждане на програми за обучение на персонала за поддържане на информационната сигурност.

Към функционалните отговорности на специалистите по информационна сигурност се отнасят някои от посочените по-горе задължения, както и:

- утвърждаване и/или участие в разработването на програма за управление на риска, необходима за осигуряване на адекватна защита на организацията при минимални разходи;
- утвърждаване и/или проверка на приетия план за информационна сигурност на всяка отделна работна (функционална) единица и работно място;
- определяне и утвърждаване на спецификации за приоритетна защита чрез разработване или модифициране на системите за заявка;
- утвърждаване и/или извършване на периодична преценка на всички системи за заявка с цел осигуряване на адекватните гаранции за защита.

Видове заплахи за сигурността на информацията

Съществуват няколко обхватни категории заплахи спрямо съхраняваната секретна информация[12]:

- случайни разкрития, промени или разрушаване на информацията поради грешки в хардуера, софтуера, случайни грешки на човешкия фактор или съчетание от гореизброените причини;

- случаен неправомерен достъп, в резултат на който се правят разкрития, изменения или разрушаване на съхраняваната информация от страна на: незапознати с техниката лица като оператори на терминали, административни служители, чистачки и др.; обучен персонал, като програмисти, системни анализатори, системни програмисти и др., които имат значителен технически опит;
- предумишлени престъпни действия;
- природни бедствия.

Както може да се установи, при всички заплахи, с изключение на природните бедствия, основна роля играе човешкият фактор. Поради това според нас вземаните мерки би следвало да включват обучение, проверки и контрол на персонала и на други лица, имащи някакъв достъп до информационните технологии.

Внедряване и оценка на мерки за сигурност

Количественият и качественият анализ на ситуацията дават основа за препоръки за мерките за сигурност. Първоначално се идентифицират заплахите, после се обмисля защитата, подборът на мерките за сигурност и възможните корекции. След като се подберат възможните мерки за сигурност, те могат да бъдат класифицирани според разходите и според времето за въвеждането им по следния начин:

- малки разходи, неотложно внедряване;
- големи разходи, неотложно внедряване;
- малки разходи, постепенно внедряване;
- големи разходи, постепенно внедряване.

При това обаче трябва да се взима под внимание и квалификацията на персонала, склонността на служителите да поемат наглед досадни отговорности за спазването на мерките за сигурност и пр.

Трудности при внедряването

Внедряването на мерките за сигурност може да предизвика промени в процесите на извършваната дейност, във функциите на отговорните лица и в отговорностите на човешкия фактор. Поради това, както при всеки иновационен процес, е необходимо да се направи всичко възможно за предварително изясняване на възможните бариери, на приоритетите при внедряването на съответната новост и на начините за преодоляване на трудностите. Пример за обстойна типология на негативните фактори при научно-техническите нововъведения се съдържа в първата монография на

автора.[13] Както се оказва, организационните и бюрократичните трудности продължават да доминират при внедряването на каквито и да е новости. В случая особено важно е отговарящите за информационната сигурност да преодолеят нагласата на служители и ръководители към бездействие и даже към противодействие (макар и като пасивна съпротива) спрямо мерките за защита. У нас има немалко хора, които по типичен български начин на мислене не допускат, че именно на тях може да се случи инцидент.

При внедряването на мерки за сигурност за избягване на рисковете би следвало да се вземат предвид следните особености.

Много от мерките за сигурност са включени при технологичното разработване на хардуера и на софтуера. Достатъчно е хората, които работят с информационната техника, да познават и спазват препоръките в печатните материали, обясняващи устройството и начина на работа с техниката.

Програмите за обучение на персонала би следвало да дават конкретна техническа информация за вземаните мерки за сигурност и същевременно да формират у хората от персонала положителна нагласа към осигуряването на безопасността в различните й аспекти.

Освен това обаче е необходимо да се има предвид, че въвеждането на нова технология, програмен продукт или назначаването на нов персонал може да доведе до нов или различен вид риск. Преценката на този нововъзникнал рисков момент би трябвало да се прави от експерти, а не да внася смут и недоверие у персонала, който при всички случай ще е недоволен (макар и негласно) от нарасналите изисквания и трудоемки процедури при осигуряването на солидни мерки за безопасност.

Полезно е провеждането на периодични съвещания, на които да се прави преценка и да се изваждат от употреба тези мерки за сигурност, които са се оказали неефективни, нефункционални, излишни от гледна точка на защита срещу новопоявили се рискове. В същото време разработваните нови технологии би трябвало да ограничават риска, допускан в досегашните технологии. В някои компютърни системи вече има "вградени" защитни програми срещу компютърни вируси, а други се конструират така, че възприемането на вируси е затруднено.

Заплахите за сигурността на информационните обекти засега не намаляват. Поради това вниманието към някои от основните компоненти на информационната сигурност, чиито проблеми ще бъдат разгледани в последващото изложение, продължава да расте.

БЕЗОПАСНОСТ, ОТНАСЯЩА СЕ ДО ПЕРСОНАЛА

Очевидно една организация, която работи предимно с информация, би трябвало да бъде структурирана така, че получаваните резултати да съответстват не само на поставените от ръководството цели, но и да задоволяват очакванията на всеки специалист и служител от организацията. Такъв е съветът на П. Дракър към предприемачите, готови да се вкопчат в "предприемаческото джудо."[14] Същевременно другото неотменимо изискване към изградената върху информацията организация е всеки специалист да поеме отговорност за безопасността на информацията не само на неговото, а и на по-ниските равнища.

Програмата за безопасност, отнасяща се до персонала (или личния състав), би трябвало да е разработена и представена от съответното ръководство. Тя трябва да изяснява възприетите критерии за определяне на степента на поверителност, спазвана от изпълнителите на съответни длъжности, равнищата на личен достъп до поверителни данни и методите за проверка на личния състав.

Тази програма трябва да предвижда такива мерки и процедури, че до специфични равнища на информация да имат достъп само верни и лоялни на институцията (фирмата, организацията) служители. При разглеждането на проблемите, отнасящи се до персонала, не трябва да се забравя, че в областите, в които се работи с микрокомпютърната техника, са привлечени много експерти и професионалисти. Проблемът е в това, че както посочват изследователите, професионалните експерти "като че ли получават удовлетворение от изпълнението на своите собствени вътрешни изисквания и от присъщото на човека задоволство от самата задача. В действителност те имат отговорност към задачата, а не към длъжността; към собствените си изисквания, а не към началника си. Те не са добри ‘служители на компанията,’ те се чувствуват ангажирани само към проблемите, които изискват от тях да разплитат трудни ситуации."[15]

В светлината на гореказаното може да се разглежда и проблемът за наемане на висококвалифицирани консултанти, изследователи и др., с каквито дадена организация не разполага в своите служби и се налага да ги привлече отвън, да ги "асоциира". При изследването на този проблем обаче Алвин Тофлър с право отбелязва, че думата "асоцииран" предполага равнопоставеност, а не подчиненост. Той изтъква, че "докато организационният човек беше покорен на организацията, асоцииранят човек е равнодушен към нея. Докато организационният човек беше парализиран от тревогата си за своята икономическа сигурност, асоцииранят човек все повече приема икономическата сигурност за даденост."[16] Тези изводи може би са валидни и за общества, които са в период на преход. Макар и заплахата от безработица да нараства, тя все по-малко плаши предприемчиви и висококвалифицирани специалисти, които не страдат от скрупули.

Длъжностите, при които се работи с поверителна информация, включват задължения, съобразени с равнището на секретност и опасността от непозволено навлизане в информационната система. С други думи, има пряка връзка между поверителните данни и поверителните длъжности.

Необходимо е ръководството да определи най-високата степен на секретност на информацията и задълженията на изпълнителите на съответните длъжности, които трябва да предотвратят неправомерен достъп и да неутрализират евентуален пробив в системите за безопасност. Естествено колкото по-висока е степента на секретност на данните и източниците, до които има достъп изпълнителят на дадена длъжност, толкова по-засекретена е тя.

Проверки на външните лица и персонала

Доколкото предварителният подбор не може да гарантира честността на служителите, налага се да се предприемат мерки за ограничаване на неправомерния достъп на неупълномощени служители, както и за решаване на други проблеми на безопасността.

Бързото приобщаване на личния състав към работата с информационни технологии прави проверката на тяхното минало и на заобикалящата ги близка социална среда все по-необходими. Съществено е да се отбележи, че на подобни проверки е необходимо да се подлагат не само идващи "отвън" кандидати за служители, а и всеки от личния състав, комуто се налага да премине от длъжност с по-ниско равнище на секретност към длъжност с по-високо равнище на секретност. Т.е. по-дълбоко засекретената длъжност изисква по-задълбочена биографична проверка.

За да се улесни въвеждането и утвърждаването на системата за безопасност, е необходимо всички служители да бъдат запознати както с необходимостта от нея, така и с печални резултати от небрежност към безопасността при работа с информацията.

Необходимо е служителите да възприемат идеята за информационната безопасност като вътрешноприсъща на всекидневната им работа. При това (въпреки че напоследък подобни идеи са бламирани) би следвало да се утвърдят и оповестят съответни стимули, които да насърчават доблестта, честността и бдителността на служителите, помогнали за разкриването на компютърни престъпления или уличаващи в отклонения от правилата за безопасност някои свои недобросъвестни колеги.

Контрол върху длъжностните лица

Традиционните проблеми в сферата на информационната сигурност възникват

главно поради неясноти при споделяне на отговорностите, поради незачитане на критичните препоръки и от съществуването на неофициални, понякога и неогласени вътрешни правила. Крос и Уотсън обръщат специално внимание на факта, че 90 % от компютърната сигурност се основава на използването на пароли. Те отбелязват случаи, при които служители са оставяли картончето с паролата не до самия компютър (което също е нарушение), а на таблото за съобщения "за да го види колегата, който поема следващата смяна."[17] Всъщност при такава безотговорност паролата става достояние на всеки случаен посетител. Поради това сигурността на системата е такава, каквато е степента на отговорност на най-недисциплинирания потребител (служител).

За да се ограничат посочените слабости, се препоръчва:

- различните отдели и служби да бъдат разделени и физически, за да се ограничава достъпът до специфична информация във всеки от тях;
- да се отдели физически компютърната техника от хората, които ползват информация, но не работят с тази техника;
- да се назначат местни служители, които да отговарят за информационната сигурност в оперативните отдели и звена;
- да се утвърди масовото участие на служителите при критичните обсъждания на програмите за безопасност;
- да се избягват ситуации, при които никой лично не носи конкретна отговорност за даден цялостен процес;
- знанията, необходими за увреждане на системата, да бъдат достъпни на минимален брой служители;
- на отговорни длъжности да се назначават проверени лица;
- при възникване на конфликти да се прилага, доколкото е възможно, ротационен принцип на работните места на служителите.

Освен това видни експерти отбелязват, че за организации, занимаващи се основно с информация, е твърде важно своевременно да се решават нововъзникналите проблеми на управлението. Сред особено критичните проблеми са:

- развитието на система за поощряване, за получаване на признание и на възможности за развитие на специалистите;
- създаването на общо виждане на специалистите в организацията (но изразено не само в декларативни изявления, а и във всекидневното професионално поведение и лоялността към организацията извън нейните стени);
- разработването на управленска структура на организацията, състояща се от

целеви групи (но не самоцелно, не за да се подражава на поредния "по-голям брат" и не поради роднински / приятелски мотиви или вследствие подтици, изяснявани от З. Фройд);

- планомерното издирване и осигуряване на висши ръководни кадри, на тяхната подготовка и апробация.[18]

Разпределяне на отговорностите

Много от проблемите на безопасността при информационните технологии възникват поради неуточнена, неясно формулирана, неадресирана или "споделена" отговорност за изпълнението на конкретни задачи. Това не е убягнало от погледа на експертите, които предлагат специфични препоръки.[19]

За осигуряване на безопасността на микрокомпютърната техника е необходимо да бъдат назначени служители, които да информират потребителите, да изпълняват и да отговарят за посочените по-долу функции:

- проверка на сигурността при автоматична обработка на данни;
- проверки на разрешенията за достъп на потребителите;
- достъпа до системи, програми и документация;
- достъпа до инструкции и ръководства;
- контрол върху данните, съхранявани в устройствата, и върху информационните носители;
- създаване и съхраняване на резервните копия;
- контакти с доставчици, сервизен персонал и др.

Необходимо е също така да се предвиди възможност за важни задачи да отговаря повече от един служител, за да има взаимозаменяемост.

В заключение още веднъж ще посочим, че ролята на човешкия фактор при осъществяване на информационна сигурност е решаваща. Независимо от постижения като чипа "Клипър"[20] все още както създаването на технологии и процедури за информационната сигурност, така (и особено) тяхното прилагане и спазване зависят от множеството програмисти, анализатори, специалисти, експерти, но и от милионите потребители. Несъмнено ускореното развитие на технологиите би следвало да се съпровожда от осмисляне и утвърждаване на съответни правни норми, които да дават гаранция за запазването на информация, свързана с достойнството и собствеността на личността и защитата на обществените и държавните интереси. Заедно с това се налага в сферите, наситени с информационни технологии, да се полагат повече усилия и за провеждане на курсове по етика и за утвърждаване на професионални етични кодекси на основата на утвърдени от вековете човешки ценности.

[1] Николай Генов, *Рационалност и социология* (София: Изд. БАН, 1986), 250.

[2] Вафа Моаед, "Международни финансови измами," Доклад пред научно-техническа конференция *Ролята на интелектуалците в условията на криза* (София, ноември 1997).

[3] Margaret Jackson, "Incidence of Computer Misuse,"in *Faculty of Business Working Paper Series* 1993/07 (Melbourne: Royal Melbourne Institute of Technology, 1993), 8.

[4] Ken Wong and Steve Watt, *Managing Information Security: A Non-Technical Management Guide* (Oxford: Elsevier Advanced Technology, 1990), 89.

[5] Христо Домозетов, *Микрокомпютри, човек, информационна сигурност* (София: Ел Ге, 1996), 25.

[6] Велизар Шаламанов и Тодор Тагарев, *Информационни аспекти на сигурността* (София: ПроКон, 1996), 77.

[7] К.К. Грищенко, "Человеческий фактор интенсификации производства", В: *Управление трудовым коллективом* (Киев: Наукова думка, 1988), 43.

[8] Това е направено, например, от А.П. Суханов, *Информация и прогресс* (Новосибирск, 1988), 86.

[9] Computer Security Research & Development. Защита на информацията в персоналните компютри, *Computerworld/България* 6 (15-21 февруари 1995), 12-13.

[10] Домозетов, *Микрокомпютри, човек, информационна сигурност*, 127-128.

[11] Robert Cross and Tony Watson, *The Professional Analyst* (Perth: Anderson Press, 1992), 158.

[12] Домозетов, *Микрокомпютри, човек, информационна сигурност*, 130-133.

[13] Христо Домозетов, *Нововъведение и внедряване* (София: Изд. БАН, 1980), 120-123.

[14] P.F.Drucker, *Innovation and Entrepreneurship* (London: Pan Books, 1986), 251-255.

[15] Алвин Тофлър, *Шок от бъдещето* (София: Народна култура, 1992), 102.

[16] Тофлър, *Шок от бъдещето*, 103.

[17] Cross and Watson, *The Professional Analyst*, 165.

[18] Питър Дракър, *Новите реалности* (София: Хр.Ботев, 1992), 217.

[19] *Data Security for Personal Files - General Recommendations* (Stockholm: The Data Inspectorate, 1990), 35.

[20] Според Ерих Шмид Еенбоом и Джо Ангерер чипът "Клипър" - малък електронен градивен елемент, който може да се вгражда в комуникационни компютри, телефонни и факс апарати - дава възможност на американското правителство и на негови институции да осъществяват контрол върху информацията, която обменят клиентите, закупили подобни устройства. Вж. *Мръсните трикове на икономическия шпионаж* (София: Атлантис, 1995), 200-203.

Christo DOMOZETOV: Born in 1941. M.Sc. (1969, Telecommunications) from the Technical University of Sofia, Ph.D. (1978, Sociology) from the Institute of Sociology at the Bulgarian Academy of Science, D.Sc. (1997, Sociology). Associated professor since 1985. Author of seven books and over 50 papers. Three of the books and over 25 articles are devoted to problems of computerization and information security. Main research interests in social problems of information technologies and innovation, as well as in military sociology. Dr. Domozetov organized and performed two international comparative surveys in the US (1989) and Australia (1993). NATO Fellow, 1992-1993. Currently works as Head Expert in the Sociological Research Center at the Bulgarian Ministry of Defense.
Fax: (359 2) 81282534; (359 2) 9888700.