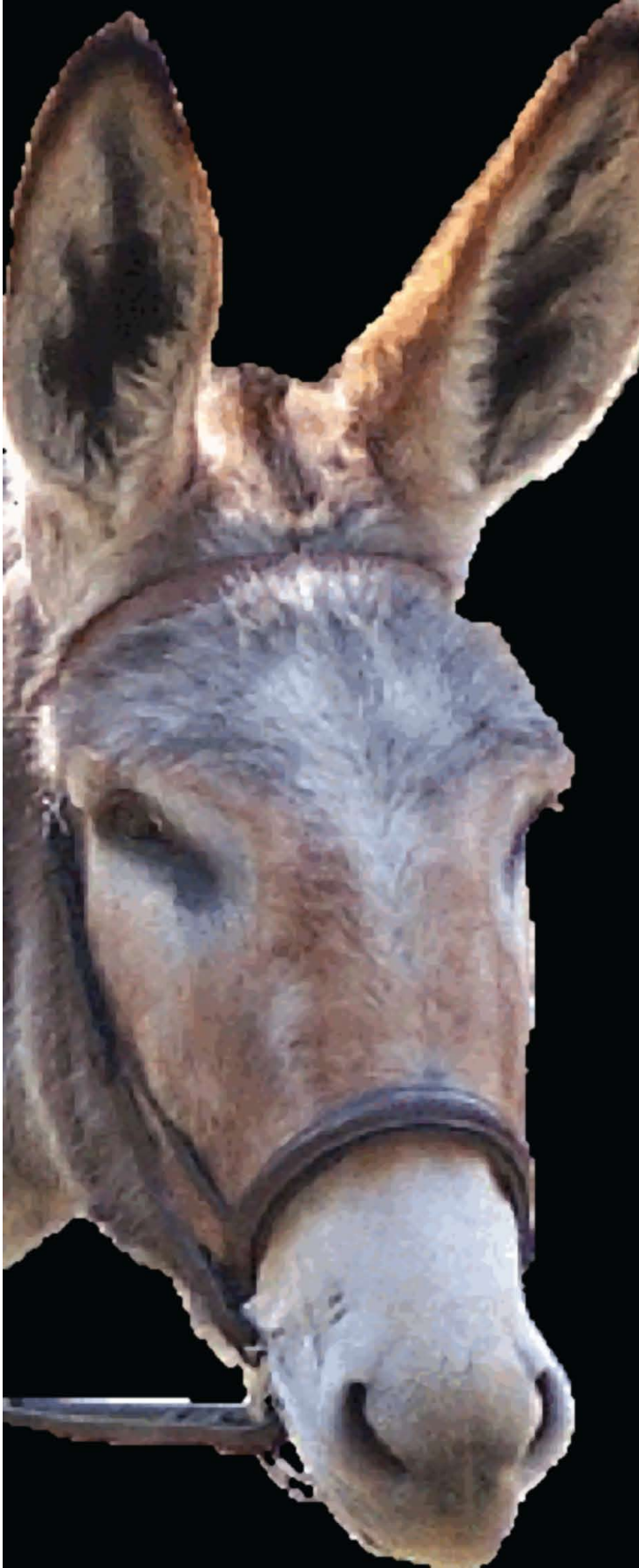
Стоян Денчев

ИНФОРМАЦИЯ И СИГУРНОСТ



За буквите
О писменехъ

Стоян Денчев

ИНФОРМАЦИЯ И СИГУРНОСТ

За буквите
О писменех

София, 2019

ИНФОРМАЦИЯ И СИГУРНОСТ

© проф. д.ик.н. Стоян Денчев, автор, 2019
© проф. д.н. Ирена Петева, проф. д.н. Стефан Симеонов, проф. д-р Стефан Мичев, рецензенти, 2019

© Павел Митков, художник, 2019
© Академично издателство „За буквите – О писменехь“, 2019
Университет по библиотекознание и информационни технологии, София, България

ISBN 978-619-185-369-4 – pdf

Stoyan Denchev

INFORMATION AND SECURITY

За буквите
Ó П Н С М Е Н Е Х Ъ

Bulgaria, Sofia, 2019

На корицата:	Идеята за композицията е реализирана от проф. Ирена Петева.
On the cover:	The idea of the composition has been realized by prof. Irena Peteva.
На обложке:	Идея композиции была реализована проф. Ирэной Петевой.

Първа част – картина	Идеята за композицията е вдъхновена от картината на Леонардо да Винчи „Джокондата“ („Мона Лиза“) – шедьовър на изящното изкуство.
First Part – Picture:	The idea of the composition has been inspired by Leonardo da Vinci's painting "La Gioconda" ("Mona Lisa") – masterpiece.
Первая часть – картина:	Идея композиции была вдохновлена картиной Леонардо да Винчи „Джоконда“ („Мона Лиза“) – шедевр изобразительного искусства.

Втора част – картина:	Идеята за композицията е вдъхновена от картината на Пабло Пикасо „Герника“ – шедьовър на изящното изкуство.
Second Part – Picture:	The idea of the composition has been inspired by Picasso's painting "Guernica" – masterpiece.
Вторая часть – картина:	Идея композиции вдохновлена картиной Пабло Пикасо „Герника“ – шедевр изобразительного искусства.

Стоян Денчев

ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ

За буквите
О писменех

Болгария, Sofia, 2019

СЪДЪРЖАНИЕ

CONTENTS

СОДЕРЖАНИЕ

ВЪВЕДЕНИЕ

В началото на XXI век новите информационни и комуникационни технологии предизвикаха глобална интеграция на информационното пространство на човечеството, като станаха основа за формиране и развитие на нови обществени отношения. Отчитайки глобалните тенденции, законодателите в световен мащаб създадоха нормативна база, уреждаща тези отношения в информационната и комуникационната сфера. В частност се въведоха ефективни механизми за гарантиране на информационната сигурност по отношение на всички субекти, които създават, обработват, съхраняват и пренасят информация с автоматизирани информационни системи и мрежи. Успешно бяха създадени и развити системи за защита на информацията, както и системи за сертифициране на средствата за нейната защита. Това формира нова регулационна рамка за гарантиране на информационната сигурност в управленски, организационен и програмно-технически аспект. Тази рамка постави на дневен ред въпроса за разработката на ефективни политики, правила и процедури за информационната сигурност в конкретните автоматизирани системи и мрежи за обработка на информация и управление.

Настоящото изследване е посветено на основния проблем на съвременната информационна цивилизация – анализа на феномена информация и неговата защита в автоматизираните информационни системи и мрежи.

Обект на изследването е информацията като нематериална същност, както и нейната сигурност в различните си социални и виртуални интерпретации.

Липсата на обща основа за моделиране на информационни процеси и тяхното адекватно представяне в контекстта на сигурността налага да се разработят обща концепция, политика и процедури, които са **предмет** на настоящото изследване.

Целта е да се формира и обоснове единна и балансирана система от принципи и мерки, осигуряващи формулирането и изпъл-

нението на задължителните общи условия, чрез които да се дефинират специфичните изисквания към феномена информация и неговата тотална доминация в рамките на съвременните обществени отношения, в контекста на тяхната сигурност.

За постигането на тази цел се решава **основната задача** за разработка на концептуален, доминантен модел на информационна среда и осигуряване на социална и виртуална сигурност и защита на информацията в компютърните системи и мрежи.

Комплексността на задължителните общи условия и специфичните изисквания към глобалната информационна среда и средата за сигурност на автоматизираните информационни системи и мрежи, разнообразието на техните компоненти и многообхватността на техните връзки предполагат необходимостта от намиране на адекватни методи и алгоритми. Ето защо синтезът и анализът на основните компоненти на информационната среда са основна част от настоящото изследване.

Работната хипотеза на настоящото изследване е, че при синтеза на концептуален модел на информационна среда и на среда за защита на информацията се изграждат артефакти, създаващи основа за развитие на нова динамична организация на събирането, съхраняването, обработката и разпространението на информацията, отговаряща на нарастващите изисквания на текущата социална практика. В този случай и при тези условия процесът на обратен информационен синтез се гарантира от практическия анализ и ефективното прилагане на политики, правила и процедури, гарантиращи синхрон на дейностите по управлението на информацията и знанията и на тяхната защита.

Това би могло да се постигне чрез:

- **активно управление**, гарантирано от наличието на достатъчни по обем и качество информация и знания, както и лидер и подходящ управленски екип;
- **управление на знанието** чрез системно акумулиране и изследване на данни и трансферирането им в използваема информация;
- **обучение**, гарантиращо натрупване и повторно използване на информация и знания, водещо до съкращаване на времето за разрешаване на стари и нововъзникнали казуси;
- **мрежов подход** – гъвкавост и интеграция, способстващи за

максимално използване на наличните ресурси независимо от дислоцирането им;

• **готовност за промяна**, способстваща за възприемане на иновациите и проактивно отношение към съществуващите възможности.

Избрана е **методика** за изследване, базираща се на т.нар. архитектурен подход, формиращ основния съвременен инструментариум на модерната методология на промяната, която включва:

• анализ на постигнатото в предметната област;

• определяне на нерешените задачи;

• избор на задачи за решаване;

• определяне на необходимия апарат за решаване на проблемите;

• алгоритмизации на програмни реализации;

• експериментиране;

• анализ на резултатите от експериментирането;

• частично (пилотно) внедряване;

• влизане на системата в реален жизнен цикъл.

Тази методика е естествена за подобни случаи, може да даде и дава отговор на предвидените и реализирани задачи в представеното изследване.

Методологията на изследването включва:

• **Наблюдения.** Изводите в настоящото изследване са направени на базата на наблюдения и проучвания на процесите на формиране и защита на информационни потоци.

• **Ретроспективен анализ.** При формулиране на изводите и препоръките е отчетено развитието на възгледите, идеите и моделите на информационната среда от възникването им до наши дни.

• **Проучване на документи.** Събрани, систематизирани и проучени са основни нормативни документи, регламентиращи обществените отношения в сферата на информационната среда и нейната сигурност.

• **Изучаване на опит.** Изучен е водещият световен опит в сферата на управлението на информацията и знанията.

• **Прогнозиране.** Чрез базиране на проучването на най-добрите световни практики, са направени изводи и препоръки за бъдещото развитие на процесите по управление на информацията и на нейната защита.

• **Събеседване с експерти.** Проведени са срещи и събеседвания с водещи световни експерти, активно работещи и прилагащи иновативен инструментариум за управление и защита на информацията.

• **Консултации.** Участието в научни конференции, семинари и дискусии даде възможност за провеждане на консултации относно изграждането на модел за ефективно управление на информационна среда.

• **Преминаване от абстрактно към конкретно.** В настоящата работа са показани възможностите за синтез на концептуални пораждащи модели, от които впоследствие се извеждат политики, правила и работни процедури, свързани с управлението на конкретна информационна среда.

• **Факторен анализ.** Формулирането на част от направените изводи и препоръки е осъществено на базата на направения анализ на факторите, влияещи върху ефективното управление на информационната среда

• **Единство на историческо и логическо.** Направено е успешно усилие натрупаният опит, специфичните културни характеристики, традицията и националните специфики да намерят отражение в процеса на адаптиране на моделите, методите и инструментариума за управление и защита на информацията в световен мащаб.

В настоящата работа изложението е структурирано в две основни части:

В първата част на настоящото изследване е представена концепцията за развитието на феномена ИНФОРМАЦИЯ. Обърнато е специално внимание на тематиката, свързана с понятията ИНФОРМАЦИОННА СРЕДА и ИНФОРМАЦИОНЕН ПРОЦЕС. Поставен е акцент върху основните постулати на НАУКАТА ЗА ИНФОРМИРАНЕ. Направен е задълбочен анализ на ролята и значението на информацията като основен ресурс на информационната цивилизация и в частност на информационното общество. Показани са фундаменталната роля на знанието за развитието на съвременатa икономика, наречена икономика на знанието, механизмите и технологиите за неговотго управление и прилагането му в текущата социална практика.

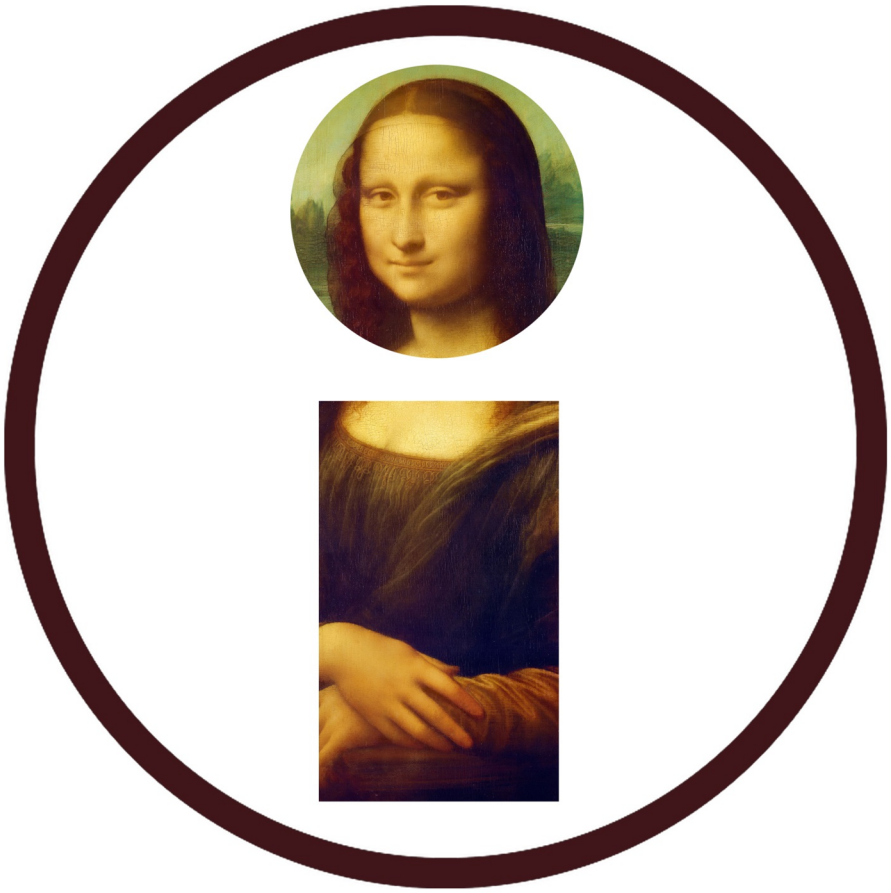
Във втората част на изследването на основата на анализ на

връзката „информационно пространство – сигурност“ е разкрита регулиращата функция на секретността. Разглеждат се политиките за защита на информацията в компютърните системи за управление Анализирани са основните положения на сигурността на автоматизираните информационни системи и мрежи и е дадено описание на управленските, организационно-техническите и програмно-техническите аспекти на защитата на информацията в тях. Дадено е кратко описание на физическата, персоналната, документалната, комуникационната и криптографската сигурност, защитата от паразитни електромагнитни излъчвания и базовите изисквания за компютърна сигурност. Описани са режимите за сигурност по време на експлоатацията и развитието на сертифицирани автоматизирани информационни системи или мрежи. Допълнително внимание е обърнато на сигурността на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява или пренася информация с високо ниво на класифицираност. Показани са съществуващите възможности и свързаният с тях риск. Разгледани са въпросите за информационната цялост, конфиденциалността на информацията, публичното представяне, правата за интелектуална собственост, контрола на достъпа, личното ползване и очаквания, докладването на проблемите със сигурността.

Фрагментарно са разгледани и анализирани някои базови компоненти на хибридните заплахи, информационните войни и в частност на „цветните“ революции. Специално внимание е обърнато и на фундаментите на т.нар. киберсигурност.

Като цяло изложените резултати могат да послужат на всички специалисти, докторанти и студенти, работещи по проблемите на информационната наука, науката за информирането, информационната цивилизация и икономиката на знанието. Монографията ще е полезна и за тези от тях, които по естествен път са разкрили основите на интеракционните процеси между информацията и сигурността и желаят да задълбочат своите познания в областта на регулиращите функции на сигурността в текущите социални, технологични, военни и политически практики.

ИНФОРМАЦИЯ



ИНФОРМАЦИОННА ЦИВИЛИЗАЦИЯ

Твърди се и ние приемаме това твърдение, че информационната цивилизация е пореден качествен еволюционен етап от развитието на обществените отношения и обществените практики. Тя се характеризира не само с тотална доминация на информацията, но най-вече с авангардните технологии за нейното използване в глобалната социална практика.

ИНФОРМАЦИОННО ОБЩЕСТВО

Теоретичните постановки на информационното общество го определят като изцяло нова обществена система, висш, съвременен стадий на развитие, нов цивилизационен модел. Трансформациите и коренните промени, настъпващи в съвременното развитие на обществото, обхващат всички сфери на живота и засягат както отделния индивид, така и цялата цивилизация. Същността на понятието „цивилизация“ може да се разглежда в различен контекст – културологичен, исторически, социологически. От гледна точка на социологията цивилизацията е система от определени обществени отношения, процеси и дейности, върховно постижение на човечеството и личността, на тяхната материална и духовна култура и поведение, съществували в определено време и оставили дълбоки следи в еволюцията на човечеството.

В основата на възникването и развитието на идеята за информационното общество като нов цивилизационен модел стои промяната като главна движеща сила на обществеото развитие. Съвременната промяна е обусловена от значението на информацията като основен ресурс за всички сфери – политика, държавно управление, икономика, образование, здравеопазване, култура. Процесът на изменения обхваща целия спектър на обществения живот, той е повсеместен и необратим. Тези изменения са многофакторни и съдържат елементи на качествен синтез на нови способи не само за възприемане на съвременния свят, но и за активно човешко участие в създаването на нова реалност. Автори като А. Тофлър, В.

М. Глушков, П. Дракър, К. Кларк, П. Кенън, М. Кастелс, Е. Фром и др. изследват процесите на развитие и промяна и факторите, които ги обуславят, привеждат неоспорими аргументи в полза на теорията за настъпващ нов етап и за развитието на нова цивилизация – информационната.

ИНФОРМАЦИОННО ОБЩЕСТВО – ВЪЗНИКВАНЕ, ХАРАКТЕРИСТИКИ И ПРЕДПОСТАВКИ ЗА ИЗГРАЖДАНЕТО МУ

Съвременното общество се характеризира с качествено ново отношение към информацията. Това се дължи на големите технологични постижения, маркирали XX век – създаването и развитието на комуникационните и компютърните технологии. Развитието на интернет показва най-добре синергичния ефект от тяхното съчетаване и илюстрира огромното значение на комуникационните и компютърните технологии за съвременното общество, което днес определяме като информационно. Само за малко повече от 20 години, от масовото навлизане на интернет в обществената практика, тази технология, този истински феномен на съвременната цивилизация намери място във всяка страна и във всяка социална система, включително в най-малката – семейството; промени по радикален начин общуването между хората; направи общо- и леснодостъпни огромни информационни ресурси; осигури глобализирането не само на икономиката, но и на всички области на социалната практика.

Впрочем напоследък (преди 13 години) възникна един куриозен, но много сериозен въпрос, засягащ бъдещето на интернет. На 22.06.2006 г. в гр. Маракеш, Мароко, се проведе работна среща на ICANN (Internet Corporation For Assigned Names and Numbers), на която бяха разисквани въпроси относно администрирането на Мрежата, тъй като на 30.09.2006 г. изтичаше срокът на договора между правителството на САЩ и ICANN. Както е известно, още със самото си създаване интернет пряко и косвено се администрира от правителствени структури на САЩ. Известна е съпротивата на редица световни фактори, в това число и Европейската комисия, срещу сегашния модел на американско доминиране в тази област.

Поддръжниците на статуквото обаче изведоха много силни аргументи, че ако в момента има известен минимален хаос, при евентуален трансфер на функциите към някоя международна организация никой няма да бъде в състояние да предвиди размера на хаоса и по какъв начин той ще се отрази на дейността на Мрежата. С проблема тогава се ангажира дори Генералният секретар на ООН Кофи Анан, който в официално съобщение декларира, че почти сигурно се планира подновяването на договора с Търговския департамент на САЩ и се подкрепя ICANN като уникална организация с отговорности по администрирането на Мрежата.

Кои са характерните белези на информационното общество?

Може би съществуват стотици, а защо не и хиляди такива. В крайна сметка основните, отличителните белези на информационното общество може да се сведат до няколко:

1. Демократично използване на информационните ресурси – достъпът до информация е не само узаконено право на гражданите, но са налице и технологични възможности мнозинството от тях да се възползват от това си право.

2. Целенасоченото търсене на информация за вземане на най-разнообразни решения, включително най-елементарните, се превърна в масова потребност.

3. Липса на силова цензура както в предлагането, така и в достъпа до информация.

Основен принцип на информационното общество е, че **достъпът до информация е основно човешко право**, а информационните и комуникационните технологии създават предпоставки за свободното му упражняване. В крайна сметка горното недвусмислено означава, че глобалните информационни ресурси трябва да се използват **ДЕМОКРАТИЧНО**. Дали в действителност това е така?

В края на 2011 и началото на 2012 г. ФБР на САЩ обаче изготви и предложи за „обществено“ обсъждане нов проект за наблюдение в интернет, който веднага предизвика остри реакции заради нарушаването на конфиденциалността на информацията в Мрежата. Федералното бюро искаше да получава достъп до информацията в интернет, без да се налага да получава съдебни решения за всеки случай на наблюдение. Очакваше се правната битка „за“ и „против“ мониторинга в

интернет да бъде доста оспорвана в Конгреса на САЩ. Тя започна, след като директорът на ФБР и конгресмени от Републиканската партия показаха план за неограничено наблюдение върху интернет комуникациите. По този повод дори Президентът на САЩ Барак Обама (2009 – 2017) направи безпрецедентно предварително изказване, че ще наложи вето върху евентуален закон, който ограничава свободите и правата на гражданите.

По време на изслушване в Правната комисия на Камарата на представителите в американския Конгрес директорът на ФБР Робърт Мълър (понастоящем назначен за специален прокурор в разследването на евентуалната руска намеса в последните президентски избори на САЩ) и конгресменът от Републиканската партия Даръл Иса представиха план, който нарекоха двустепенен подход. Първата стъпка на този план включва въвеждането на изискване към доставчиците на интернет (ISP) да предоставят на ФБР доброволно достъп до мрежите си. Втората стъпка е приемането на федерален закон, който задължава интернет компаниите да сътрудничат на ФБР.

Аргументът на ФБР за това е, че така ще се предотвратяват всякакви кражби на лична информация и използването ѝ за извършване на престъпления. Бюрото за разследване твърди още, че мониторингът в интернет ще помогне да бъдат разкривани редица престъпления, сред които кражбата на секретна информация. Според Мълър „законодателството трябва да бъде усъвършенствано“ и един нов законо трябвало да дава на службите за сигурност повече възможности да идентифицират лица, които извършват незаконни дейности.

Опитът на ФБР да узакони почти неограниченото наблюдение в интернет от службите за сигурност, не е само американски феномен. Той най-вероятно ще има глобално въздействие и ще даде правни аргументи на много правителства да засилят контрола върпу комуникациите в интернет.

Приемането на идеите на ФБР означава, че правителството ще може да прави възможно най-дълбочинни изследвания и пълен мониторинг на поведението на интернет потребителите. Всъщност такива вече се прилагат, но от частни компании. Американската компания КОМКАСТ (COMCAST) следи дали клиентите ѝ използват технологията „Бит торент“ (Bit Torrent) за обмен на данни в интернет. Британският интернет доставчик „Форм“ (Phorm) също

следи поведението на потребителите си в интернет.

Според американските медии нито републиканският конгресмен Даръл Иса, нито директорът на ФБР признават, че първата стъпка от плана им за наблюдение в интернет би била незаконна.

„Има съществен проблем в предложението на Мълър", твърдеше Ал Гидари, съдружник в правната кантора „Пъркинс Койе", която защитаваше интересите на телекомуникационните компании срещу правителството. „Той забравя, че отделните щати имат правомощия да приемат по-рестриктивни закони за определени дейности и 12 от тях имат такива. Той забравя също, че живеем в глобален свят и че останалата част от него следи как ще разрешим настоящия въпрос. Голяма част от клентите ни са от страни в Европейския съюз. Те няма да харесат разширеното наблюдение, а може да се окаже и че то е със съмнителна законност", казваше още Гидари.

Ако все пак ФБР беше заставило интернет доставчиците да предават исканата от тях информация, то доставчиците щяха да бъдат принудени да нарушат Закона за неприкосновеност на електронните комуникации ECPA.

Въпреки че е приет през 1986 г., той все още е в сила. Според неговите разпоредби комуникация на определен потребител може да бъде огласявана или предавана на трето лице или инстанция само при изрично съгласие от негова страна.

Така, ако даден потребител реши да заведе дело, той ще може да осъди не само доставчика си, но и ФБР. Той ще може да обвини Бюрото, че нарушава Четвъртата поправка на Конституцията на САЩ, която забранява необоснованите разследвания.

Всичко това означава, че със сега действащото щатско и федерално законодателство ФБР може да си навлече сериозни неприятности, ако реши да следи потребителите в интернет. Очевидно, за да може да прави това, трябва да бъде променен изцяло пакетът от закони, регламентиращ следенето и разузнаването в САЩ.

Директорът на ФБР обаче беше категоричен, че Конгресът трябва да намери начин и да позволи на Бюрото да действа срещу незаконните и обществено опасни дейности още преди те да бъдат реализирани.

Явно, че битката в това направление се очертаваше да бъде жестока и безкомпромисна. От нейния изход в голяма степен зависеше не само бъдещето на глобалната мрежа, но и бъдещето на ин-

формационната цивилизация. **Видимо ФБР „загуби“ битката, но войната все още не е приключила.**

Като ефект от масовото предлагане на информация и масовия достъп до използване на технологии, улесняващи достъпа до информация, хората се оказаха залети от „информационен потоп“. Човешките възможности и умения за боравене с такъв огромен ресурс и полезното му използване се оказаха ограничени. Достъпът до прекалено много информация, която хората не могат да осмислят и да извлекат полезното знание от нея в рамките на разумен отрязък от време, има същия ефект както липсата на информация.

Влиянието на информационните технологии в икономическата сфера – както при управлението на бизнеса, така и за осъществяването на бизнес трансакции, доведе до появата на термини като „дигитална икономика“, „дигитална компания“ или съответно „интернет икономика“. Терминът „дигитален“ (цифров) произлиза от наименованието на технологиите за работа с дискретна информация, върху които се базират съвременните компютри (за разграничаване от съществуващите аналогови изчислителни машини).

„**Дигиталната икономика**“ акцентира върху бизнес модели и стратегии, станали възможни благодарение на интернет, на променените начини на производство (безлюдни технологии), директно обслужване на клиенти (*client relationship management* – CRM), електронна търговия (*business to customer* – B2C, *business to business* – B2B) и т.н.

Основните характеристики на информационното общество се формират през 60-те и 70-те години на XX век. Бурното развитие на информационните и комуникационните технологии през последните десетилетия на XX век предизвиква съществени изменения в методите и средствата за производство. Създават се нови продукти и услуги и в крайна сметка се налага цялостна промяна в структурата и функционирането на обществото. Промяната води до изграждане на качествено нови модели, връзки и взаимоотношения във всички сектори и дейности на обществото. Основните параметри на промяната са определени в три насоки:

1. Преход на икономическите и социалните функции от капитал към информация (всеки материален ресурс в крайна сметка може да се превърне в информация).

2. Нивото на знание постепенно и трайно измества собстве-

ността като фактор за социална диференциация.

3. Наличие на симбиоза между социалните организации и информационните технологии.

Нека да разгледаме някои основни тенденции в световното развитие, довели до коренната промяна на обществените отношения. До средата на XX век информацията представлява спомагателен, обслужващ ресурс в общественото производство на фона на традиционните ресурси – земя, труд, капитал. С интензификацията в развитието на производството през втората половина на миналото столетие и с нарастването на потреблението се появява дефицит на ресурсите земя и труд. Земята е немобилен ресурс, а трудът е инертен и с оскъпяваща се мобилност. Информационните и комуникационните технологии в своето развитие и усъвършенстване разкриват огромния потенциал на информационните ресурси, превръщат ги в равностойни на традиционните, а в развитите икономики те вече стават водещи, основни ресурси. В производството и разпространението на информационни стоки и услуги се влагат огромни материални и финансови ресурси и се ангажира значителна част от икономически активното население. Обособява се сектор „информационна индустрия".

Развитието на информационното общество се свързва не само с възможностите за натрупване и преработка на информацията, но и с развитието на системите и формите за комуникация. Според Т. Парсънс, главен изследовател на направлението на социологическия структурен функционизъм, комуникацията има огромно значение. Тя е метод, посредством който се предизвика действие в различните части на системата, а така също тя е средство за контрол и координация. Системата на комуникациите образува строежа, конфигурацията на организацията. Изграждането на съвременна глобална комуникационна система се възприема като основна предпоставка за развитието на информационното общество.

Анализът на особеностите на съвременната промяна дава основание на А. Тофлър да очертае измеренията на бъдещата (вече сегашната) информационна цивилизация. Централен ресурс при нея е информацията, която може да се използва от всекиго и по всяко време. Тофлър формулира две основни групи принципи, характеризиращи информационното общество, които предполагат изграждане на нова политическа структура, изискваща децентра-

лизация и по-широко и демократично участие на обществените субекти в процеса на промяна.

Същността на информационното общество като нов стадий на развитие и съществуване на обществената система намира отражение в множество публикации, изследвания и официални документи през последните години. Тази същност определя основните белези, с които то се характеризира:

– в информационното общество най-голямо значение имат информацията, знанията и технологиите;

– в информационното общество преобладава умственият труд;

– използване на информационните и комуникационните технологии във всички икономически и социални сфери;

– социалните и икономическите процеси се демасовизират;

– висока заетост в сферата на услугите;

– непрекъснат процес на обучение (обучение през целия живот);

– икономическа, политическа и социална глобализация (глобализация в областта на културата не е допустима).

Нека още веднъж да повторим казаното по-горе: **основен принцип** на информационното общество е, че **достъпът до информация е основно човешко право**, а информационните и комуникационните технологии създават предпоставки за свободното му упражняване.

Наличието или отсъствието на съвременни компютърни и комуникационни технологии е значим индикатор за степента на проблема „цифрово неравенство“. По-голямата обществена наситеност с компютърни и комуникационни технологии създава предпоставки за прехвърляне на мостове между „цифрово задоволените“ и „цифрово незадоволените“ обществени групи. Една от възможностите за преодоляване на това неравенство на сегашния етап от развитието на информационното общество е персонализацията на компютърната техника още от най-ранна детска възраст. Това означава да се осигури достъп на всяко дете, независимо от неговото местоживеене, до преносим персонален компютър, който да има постоянна връзка с интернет. За реализацията на тази идея напоследък в света се работи много усилено. През януари 2005 г. Никълъс Негропонте – ръководител на Медийната лаборатория на Масачузетския технологичен университет – САЩ (MIT Media Lab), на срещата на Световния икономически форум (WEF) в Давос,

Швейцария, направи амбициозно предложение към световната компютърна гилдия да произведе и предложи на пазара нискостойностни (до 100 долара) преносими компютри, които да бъдат на разположение на всяко дете на ученическа възраст във всяка точка на земното кълбо. Негропонте и неговите съратници създадоха некомерсиална организация, наречена OLPC (One Laptop per Child), която е подкрепена от някои от най-големи компютърни софтуерни компании (като например Google). Основната цел на сподвижниците на идеята за „100-доларови компютри", изразена от Генералния секретар на ООН Кофи Анан на Световната среща по проблемите на информационното общество в Тунис, се резюмира в думите му: „всеки един, където и да е, трябва да има възможности да споделя и да се възползва от преимуществата, които съвременните информационни технологии предоставят". Вече формално може да се твърди, че тази задача е изпълнена – бяха разработени и масово на пазара се предлагат нискостойностни компютри, но за съжаление, по същество те не решават поставените от Негропонте проблеми.

Преходът към информационно общество е съпроводен с множество негативни фактори: страхове, кризи, тероризъм, недоверие към ролята на институциите. Коренната промяна на устоите, на които се уповава човек, води и до коренна промяна в поведението и приспособимостта му към заобикалящата среда. Човешките измерения на промяната са не по-малко съществени от технологичните, икономическите и политическите. [35] Социалната дезинтеграция на отделния индивид или на дадена обществена група може да доведе до тежки последствия за цялата обществена система.

Глобализацията в икономическите, финансовите и технологичните системи, обусловена от развитието на информационните и комуникационните технологии, е друга характерна черта на новата обществена структура. Тя поражда и много въпросителни относно запазването на идентичността на отделни държави и региони и увеличаването на разликата между информационно „богати" и информационно „бедни", наречена „**дигитално разделение**".

Въпросите, осветляващи темата за публичния достъп до информация, са много мащабни и засягат основите на световното обществено-икономическо развитие. Без да се спираме в детайли на политическите и икономическите причини за появата и разви-

тието в световен мащаб на феномена ***информационно неравенство***, от гледна точка на съвременното информационно общество той представлява ***нарушена обществена комуникация***. Според нас истинските причини за експанзията на този феномен се крият в неправилното дефиниране на понятието ***ГЛОБАЛИЗЪМ*** и неговата практическа интерпретация. Ние мислим, че глобализмът е иманентна, неразделна част от политико-икономическото развитие на света. Глобализмът в политиката и икономиката не само че е възможен, той е необходима съставка за ускоряване на развитието на обществените отношения. Противници сме на антиглобалистките движения и техните отчаяни опити да спрат хода на естественото развитие на обществото. Категорични противници сме обаче и на онези, които мислят, че идеите и практиките на глобализма освен за политиката и икономиката трябва да се прилагат и за културата. Действията на такива хора и определени политически кръгове със световно влияние стоят в основата на нарушената обществена комуникация.

Ако вземем за пример Република Турция, бихме могли да забележим, че навсякъде домакините любезно предлагат на гостите си домашни чехли с презумпцията, че те ще си събуят обувките, влизайки в домовете им. Ето това е типичен пример за бита, за специфичната култура на определена група от хора, които изповядват еднакви или близки ценности. Тези културни традиции са се формирали под влиянието на различни фактори векове наред. Друг типичен пример в това отношение е нежеланието на индийците да се ръкуват. В тези два случая, съвсем опростенчески погледнато, глобализацията в областта на културата представлява влизането с обувки в домовете на турците и стискането на ръцете (здрависването) на индийците. Някои от нас биха могли да кажат „И какво от това? Какво толкова е станало?“. Напротив, станало е нещо голямо. Нещо необичайно. Нещо, противно на установените от векове традиционни обществени отношения. Нещо, което води до реакция, до съпротива. Според нас няма нужда да продължаваме да развиваме тази теза. Екстраполацията на горните мисли показва, че тенденцията тук е ясна.

Глобализацията в областта на културата води до необратими обществени и цивилизационни нарушения и задача на обществото като цяло е да намали до минимум както нейното негативно влия-

ние върху естествения ход на историята, така и непосредствените ѝ въздействия, носещи с нищо неоправдани човешки трагедии, духовни разрушения и перманентен страх.

Умният политик, умният общественик знаят, че **нещо се е случило тогава и само тогава, когато то е станало публично достояние**. Тази проста, но изстрадана максима стои в основата на обществените комуникации и дава основание т.нар. информационно съсловие (а не само журналистите) с право да бъде определяно и наричано „четвърта власт".

От гледна точка на теорията на информационната среда може да се твърди, че **сложността на една обществено-политическа система е пропорционална на количеството информация, необходимо за нейното пълно описание**. За да се разреши тази сложност, т.е. да бъде обществото напълно информирано, чисто формално погледнато, горното определение не само дава право, но и изисква от хората, които боравят с публична информация, да разкриват всичко, което се случва в рамките на глобалната информационна среда. Да, теорията е такава. Но каква е практиката?

Преодоляването на негативните явления, съпътстващи процесите на глобализация, и целенасочените дейности към адаптация в съвременните условия и интеграция в процеса на промяна на всеки човек или общност се превръщат в ключов фактор за успех при изграждането на информационното общество.

Маркираните основни тенденции в общественото развитие и съпътстващите ги проблеми са определящи при разработването на концепции и ръководни документи, формиращи стратегии и тактики за управление при настъпването на новата информационна ера в развитието на света. Ориентировъчна база за всички държавни документи е **Окинавската харта за глобалното информационно общество**. В Европа се говори за „европейски модел" за информационното общество като изходна позиция в процеса на глобализация. През 1994 г. Европейският съюз приема план за действие, наречен „Европейски път към информационното общество". Изграждането на **информационно общество като общество, основано на знанието**, е приоритет за Европейската общност. Въпреки че преходът към информационно общество е пряко обвързан с процесите на глобализацията, спецификата в развитието на всяка държава или регион определя конкретната национална

или регионална политика. За осъществяването на прехода няма точно зададени алгоритми. По тази причина всеки индивидуален модел се съобразява с конкретни особености – степен на развитие на гражданското общество, степен на развитие на комуникационната и информационната инфраструктура, културна специфика. Особено значение имат възможностите, които се предоставят на хората, да се приспособят към новите изисквания на обществената среда. Държавните институции са тези, които гарантират законодателното уреждане, създават политики за стимулиране на проекти с общонационално значение и предпоставки за активно участие на частния сектор и неправителствените организации в развитието на различни области на информационното общество.

ИКОНОМИКА НА ЗНАНИЕТО. СЪЩНОСТ, ЦЕЛИ И ТЕНДЕНЦИИ

Формирането и в крайна сметка наличието на **икономика, основана на знанието**, се определят като стратегически приоритет в политиката както на развитите, така и на развиващите се страни. Концепцията за икономика на знанието приема като изходна теорията за информационното общество и по много признаци се родее с нея. Всъщност изграждането на информационно общество е тясно преплетено с изграждането на икономика на знанието. Преди да бъдат разгледани основните характеристики и тенденции, които се асоциират с развитието на икономика на знанието, трябва да се подчертае, че общото разбиране за важната роля на знанието в икономиката не е нещо ново. Развитието на производството например винаги се е основавало на различните форми на знанието. За ролята на науката като фактор за преобразуване на производствената дейност се говори още през XVII век. Но представените в изложението дотук тенденции в развитието на обществото дават основание да се говори за новата роля на знанието като феномен на последните десетилетия. В „Новата цивилизация“ А. Тофлър и Х. Тофлър определят новата „икономика на интелекта“, при която знанието става заместител както на ресурси, така и на транспорт. Тенденциите към коренна промяна във всички обществени сфери, базирани на значението на знанието като ресурс, формират фундамента на икономиката на знанието:

– Знанието се превръща в най-значимия фактор на производството;

– Все по-голяма става ролята на човешкия капитал и в частност на образованието през целия живот;

– Развива се сервизната икономика, т.е. увеличава се делът на сферата на услугите и значително нарастват „знаниеемките“ услуги за бизнеса;

– Нараства ролята на информационната инфраструктура и информационните технологии;

– Иновациите стават ключова характеристика на икономиката и основна форма за превръщане на знанието в благосъстояние;

– Политическите и деловите кръгове осъзнават ключовата роля на иновациите и важността на знанието за развитието на икономиката и осигуряването на конкурентоспособност.

И все пак какво означава „икономика на знанието“? Като за всяко ново понятие и за „икономика на знанието“ не съществува еднозначно тълкуване на смисъла и значението му. Навремето същият проблем съществуваше и относно еднозначното определяне на понятието „информационно общество“. Въпреки това с развитието на обществото такива понятия намират дефинитивна еднозначност. За целите на нашия анализ и обобщавайки възгледите на различни изследователи, една работна версия на понятието „икономика на знанието“ би могло да изглежда така:

Икономиката на знанието е нов подход към икономическите реалности, при който знанието се превръща в основен ресурс на развитието.

Учените стигат до концепцията за икономика на знанието, изхождайки от идеята за фундаменталната промяна на значението на знанието за обществото. Тази промяна има няколко аспекта:

– знанието се определя като най-важен ресурс в обществото;

– променя се важността на ролята на кодифицираното знание за икономическата активност;

– развиват се информационните и комуникационните технологии, позволяващи по-лесно и по-евтино кодифициране, съхранение и разпространение на знанието.

Обединяването на усилията за създаване на нов подход в анализирането на развитието и промяната на икономиката води до създаването на концепцията за икономика на знанието. Тя се прев-

ръща в основен инструмент за моделирането на по-ефикасна икономическа политика и нарастването на шансовете за икономически растеж.

Карл Далмън, директор на програмата „Знание за развитие“ към **Световната банка**, дава следното определение на понятието „икономика на знанието“:

„...икономика, при която иновационните процеси – производство, преобразуване, разпространение и практическо приложение на знанието – се превръщат в главна движеща сила на социално-икономическото развитие“.

На базата на структуриране на връзката „знание – икономическо развитие“ Световната банка разработва аналитичен модел на икономиката на знанието. Определени са нейните съставящи, основни „четири стълба“.

На първо място това е **иновационната система** – от нейната ефективност зависи интегрирането на знанието в пазарните отношения. Тя е механизмът за разкриване на новите технологии, които най-пълно да задоволяват човешките потребности с наличните ресурси.

На второ място е **икономически и институционален режим**, който да способства за все по-ефективното използване на ресурсите, да стимулира експериментирането и търсенето на нови знания и да ускорява създаването на нова продукция.

На трето място са високото равнище на **образованието** на населението и **квалификацията** на кадрите. Икономиката на знанието променя изискванията към системата на образованието, така че да се създават възможности и умения за бързо усвояване на ново знание.

На четвърто място е **динамичното развитие на инфраструктурата** за обработка, съхранение и трансфер на информацията.

Поради характера си информационните и комуникационните технологии са „най-изпъкващият“ продукт на икономиката на знанието и може би по тази причина често се отъждествяват с нея.

Специалистите от Световната банка разработват 76 конкретни количествени и качествени показателя за измерване на икономиката на знанието, така че да се оценят мястото и готовността на отделните страни. Върху основата на най-важните от тях се формира общият индекс на икономиката на знанието.

Разглеждайки основните постановки за изграждането на глобал-

но информационно общество и радикалните промени, протичащи в световен мащаб, ще акцентираме върху европейските измерения на тези промени на икономическата и социалната ситуация, отразени в проекта **„Електронна Европа“ (eEurope)**. Проектът е създаден през декември 1999 г. и има за цел да ускори влизането на обединена Европа в новата икономика на знанието. По същество **eEurope** има за цел облагите от информационното общество да стигнат до всички европейци и промяната да бъде възможност за интеграция, а не заплаха. В проекта се поставя задача последиците от информационната революция да бъдат от полза за всеки член на обществото.

Формулирани са ключови принципи за постигане на целите на проекта и приоритетни области на действия, основни сред които са:

- осигуряване на повече и по-бърз и безопасен достъп до интернет;
- инвестиции в хората и знанията;
- поощряване на използването на интернет.

Заедно с приемането на програмата „Електронна Европа“ през 2000 г. са представени и параметрите, по които ще се оценява изпълнението на програмата. През 2002 г. в актуализирания план за действие **„eЕвропа 2005: Информационно общество за всички“** е поставена целта европейската икономика да се превърне в най-подготвената и конкурентоспособна в световен мащаб икономика, готова за новите условия на информационната ера. Като цяло програмата е насочена към предлагането на модерни онлайн обществени услуги, включващи изграждането на е-правителство (e-Government), е-обучение (e-Learning), е-здравеопазване (e-Health), както и на динамична бизнес среда, достъпни чрез засиленото разпространение на широколентов достъп на конкурентни цени и изграждането на сигурна информационна инфраструктура. Неразделна част от програмата **eEurope** е и стратегическият план **eEurope+**, който обхваща страните кандидатки за членство в ЕС.

ИНФОРМАЦИЯТА КАТО ОБЩЕСТВЕНО ДОСТОЯНИЕ. ЦИВИЛИЗАЦИОННИ АСПЕКТИ

Определено трябва да кажем, че в известен смисъл този и следващият раздел разширяват и дават нова трактовка на вече направени в предходните части на труда и в предходни изследвания

анализи. От формална гледна точка използването на такъв подход не е някаква новост, но по същество в тези раздели се задълбочават изследванията, които, без претенции за абсолютна изчерпателност, разкриват философската интерпретация на понятието „информация", неговите базови характеристики и развитието на съвременната цивилизация, която по своята същност се изгражда върху основата на информацията и на знанията.

Цивилизационните аспекти на достъпа до информация се определят в голяма степен в областта на правото на информация на хората като общност и на отделните индивиди като един вид гаранция за правната защитеност на личността въобще. Само свободното „движение" (на информация, знания, социален опит, иновативни умения и др.) при социалните комуникации и връзки може да гарантира независимост на гражданина от държавните структури и заедно с икономическата самостоятелност, която предполага правото на собственост, да се създадат по-добри възможности и гаранции за удовлетворяване на интересите му.

ПРАВОТО НА ИНФОРМАЦИЯ В СИСТЕМАТА НА ЧОВЕШКИТЕ И ГРАЖДАНСКИТЕ ПРАВА

От гледна точка на системата от човешки права, която на базата на историческото развитие на проблематиката определя три поколения права на човека, правото на информация се причислява към т.нар. трето поколение. То се смята за неделимо и пряко обвързано с другите права на човека. В същото време то е и фактор за реализация на немалка част от тях. По тази причина, за да бъде разбрана неговата същност, е необходимо да се познават както концепцията за правото на информация, така и процесите, довели до възникване на идеята за правата на човека като цяло. Независимо от това, че концепцията, теорията и практиката, свързани с човешките права, са обект на множество изследвания и анализи, ще направим кратка ретроспекция на историческата еволюция на идеята за правата на човека.

За първи исторически сведения, свидетелстващи за начало на идеята за правата на човека в древността, се смятат Кодексът на Хамураби – цар на Вавилон, управлявал през 2000 г. пр.н.е., и Хартата на Сирий (Кир) Велики. В тези първи писмени свидетелства са отразени първоначално признание и защита на правата, които

днес наричаме право на свобода и сигурност, свобода на придвижване, право на собственост и др.

Развитието на човешката цивилизация дава основание в елинистичната философия природният закон, разумът, равенството и достойнството на човека да бъдат определени като стойности, стоящи над държавата, а по тази причина те трябва да бъдат защитени, включително от нея.

Съвсем естествено идеята за правата на човека претърпява бурно развитие в периода на Ренесанса, през епохата на Хуманизма до Просвещението. През тези периоди на промяна в общественото развитие правата на човека от абстракция еволюират в конкретни учения, философии, теории и юридически актове.

Англия е родината на първите юридически извори в съвременния смисъл за правата на човека. Самият термин „права на човека“ принадлежи на Джон Лок. Най-известният документ през този период е знаменитата Magna Charta Libertatum – Великата харта на свободата, 1215 г. Правното учение обосновава тезата, че правата на човека са вродени, естествено присъщи. Той се ражда с тях, има си ги и правата са неотделими от него като човешко същество. Тези права са свързани със самото му съществуване. Естествените права на човека се формират извън влиянието на държавата и в този смисъл не зависят от нея. Те не са определени от страна на държавата или неин орган, но рано или късно държавата ги признава. Като непризнати от държавата естествени права на индивида, те са идеи на политическото и правното съзнание. Признати от държавата, те вече стават елемент на позитивното, писаното право (национално или международно).

Независимо че са обект на правото, по дълбоката си същност правата на човека са социално, а не юридическо явление и се считат за естествено и екзистенциално присъщи на човека. Като такива, те са неотчуждаеми и неотменими. Постфактум правата на човека стават юридическо явление, когато държавата ги признае и ги закрепи в закона. Така тя се ангажира и с тяхната защита.

В ретроспективен план, като законово установени, индивидуалните изконни права на индивида получават позитивна уредба след Пуританската революция в Англия. През 1628 г. се приема Петицията за правата, съгласно която кралската власт е ограничена от индивидуалните права и свободи на поданиците на краля. Петицията за правата включва граждански и политически права и свободи, определяни

днес като класически, или права и свободи от първо поколение.

През 1679 г. се приема Habeas Corpus Act (буквално означава „да разполагаш с тялото си“). Той урежда правното положение на лицето, намиращо се под стража и преди да е дадено на съд. Този акт предвижда гаранции против незаконния арест, срокове на съдебни процедури и други правила от групата на съдебните права.

Първите английски юридически актове по правата на човека имат практически и конкретен, макар и фрагментарен характер. За система е все още трудно да се говори, като правата се определят повече негативно, като ограничение на властта, т.е. какво тя не може да прави. В историческото си начало правата и свободите са били предоставяни само на привилегированите, но по-нататъшната им еволюция е на принципа на универсализма.

Принос на Франция в изграждането на системата от човешки права е Декларацията за правата на човека и гражданина от 1789 г. Декларацията е най-известната прокламация на правата на човека и с най-дълготрайни последици на Европейския континент.

Декларацията провъзгласява по съвременен начин презумпцията за невинност, правото пред закона, свободата от задържане, сигурността срещу обратното действие на закона, свободата на словото, печата, манифестацията, неприкосновеността на частната собственост. Впоследствие заложените в Декларацията права се развиват в конституцията и други юридически актове както във Франция, така и в конституциите на другите европейски държави, които разширяват т.нар. кръг на основните права и свободи.

Принос на САЩ във формирането на системата от граждански права и свободи е Декларацията за независимостта на САЩ (4 юли 1776 г.). В нея са закрепени правото на живот, правото на лична свобода, правото на стремеж към щастие. Друг принос е т.нар. *Бил (Закон) за проявата*, като под това наименование са известни първите десет поправки към Конституцията на САЩ. Основното в тях са свободата на словото, неприкосновеността на жилището, забраната на произволните арести.

Правата на човека и правата на гражданина са фундаментални конструкции, които не са тъждествени. Биологично това следва от разграничението между човека и гражданина, между естественото и гражданското състояние на индивида, между естественото и позитивното право.

Правата на човека са естествени права – онези права, които индивидът има по природа и които са неотделими от него като човешко същество.

Правата на гражданина са онези права на индивида, които идват от обществения договор, от връзката на индивида с една държава, от нейните закони в позитивното право. Това са възможности, които индивидът има в качеството си на гражданин и са пряко свързани с организацията и функционирането на държавата.

Понятието „права на човека“ изразява универсалната ценност на човека без оглед на неговото гражданство, т.е. на човека като такъв. Правата на гражданина го характеризират като принадлежащ към определена държава. Докато правата на човека са универсални (всеобщи), то правата на гражданина са строго национални. Правата на човека се съдържат в универсалните инструменти, но винаги международни, а правата на гражданина са винаги закрепени в националното законодателство.

В литературата еволюцията в областта на правата и свободите на човека се представя с помощта на споменатата вече концепция за т.нар. три поколения права на човека.

Първото поколение се оформя в периода на буржоазните революции и обхваща класически права и свободи, т.е. гражданските и политическите права и свободи, провъзгласени от тях. Тази група права позволяват на човека да се брани срещу произвола на държавната власт, като поставят граници на властта (избирателните права, свободата на словото).

Второто поколение права са икономически, културни и социални права и свободи. Те се обособяват с възникването на идеята за социалната държава, т.е. държава, която има определени ангажименти към своите граждани и предприема позитивни действия за изпълнение на тези ангажименти.

Третото поколение права се свързва с промените, настъпили през XX век и продължаващи и през XXI век. В него влизат две подгрупи права:

1. Вследствие на развитието на информационните и комуникационните технологии и науката в частност, се обособяват и развиват правото на достъп до информация, на екологична жизнена среда, на ненамеса в частната собственост.

2. Колективни права, които са групови и противостоят на правата на отделния индивид – право на самоопределение, право на развитие на малцинствата и др.

Концепцията за трите поколения права на човека отразява обогатяването, разширяването на темата в хода на историята. При появата на всяко следващо поколение предходното не изчезва – напротив, те се допълват, като се смята, че днес всички права в пълен обем са нужни за пълноценния живот на личността. Нещо повече, в настоящия момент, в контекста на развитието на информационната цивилизация и възникващите нови заплахи за личността, правната уредба на тази материя търпи непрекъснати промени с цел усъвършенстване и постигане на защитата им спрямо предизвикателствата на съвременния свят.

В контекста на казаното дотук смятаме, че е необходимо да се разгледа по-подробно ролята на информацията и знанията за реализацията на правата на човека. Действително както информацията, така и знанията играят първостепенна роля при реализацията на третото поколение права и свободи на човека. Например правото на собственост не би било пълноценно осъществимо в условията на неопределеност и отсъствие на необходимите знания. Или, ако вземем за пример правата на потребителите, как може да се реализират без информация за качествени и некачествени стоки, сертифицирани продукти или услуги без реклама или антиреклама или без знание за нормативната уредба, регламентираща сигурността на тези права. За целите на сигурността, при защитата на тези права се организират информационни служби и се създават банки от данни. Но за да е ефективно използването им, е необходимо гражданите не само да бъдат информирани за тяхното наличие, а да имат и достатъчна информационна култура, за да се възползват от информацията (наличие на информационна прозрачност).

Политическите права и свободи, правото на непосредствено участие в управлението на обществото и държавата, избирателните права, свободата на изразяване и т.н. са права, които също зависят в голяма степен от информацията и знанията. Именно с помощта на пълноценна информационна среда се създава основа за ефективни решения, приемани на референдуми – в процеса, при който гражданите сами формират правото. Така те встъпват в ролята на правотворчески орган, който, естествено, както и всеки друг подо-

бен орган, е длъжен да използва или да оперира с изключително достоверна и достатъчна информация и адекватни на конкретната обществена среда знания.

В контекста на казаното дотук може да се направи изводът, че правото на гражданите на информация не само не е просто субективно право, но се състои от редица юридически регламентирани обективни права. Сред тях на първо място трябва да се подчертае правото на безпрепятствено запознаване с всички законодателни и нормативни актове. Освен това универсалното право на информация на гражданите може да включва следните конкретни правомощия:

1. Право да се знае за наличието и функционирането на всички информационни системи, които в някаква степен засягат личния живот на гражданина или информация за него, а така също информация за други сфери от жизнената му дейност;

2. Право да се дава съгласие за събиране на лична информация за социално-икономическите, културните и други социални интереси и цели;

3. Право да се проверява достоверността на такава информация и да се оспорва недостоверната информация както по административен, така и по съдебен ред;

4. Право на достъп до такава информация с цел проверка и получаване на справки;

5. Право да се знае как се използва такава информация;

6. Право на информация за околната среда;

7. Право на достоверна финансова информация; и др.

За реализацията на тези права различни фактори, като информационна и комуникационна компетентност, достъп до информация, достъп до технологии и интернет, са от критично значение. Тези права са пряко зависими от рискове и заплахи, свързани с натрупването на все по-големи масиви от данни и развитието на възможностите за достъп до тях (включително неправомерен). Все по-често изискванията към демократичното управление за откритост и прозрачност, както и масовото използване на дигиталното пространство за комуникация поставят въпроса може ли прозрачността да се превърне в заплаха за демокрацията. Това е така поради факта, че колкото повече се увеличават възможностите за достъп до информация и знания, толкова повече стават и риско-

вете за неправомерното и недобронамереното им използване.

Правото на информация и на неприкосновеност на личния живот гарантират, че хората могат свободно да изразяват своето мнение и да действат в рамките на това, което се допуска от законодателството и обществените норми, а ИКТ предлагат по-широки възможности за реализация на тези права. В същото време реализацията на е-правителство и е-управление при определени условия може да доведе до ограничаване на това право. Често страхът от липсата на поверителност, от друга страна, е фактор за негативна настройка и отказ от използване на възможностите, технологиите и услугите, предоставяни от управленските органи чрез електронното правителство или електронното управление. Неприкосновеността на личния живот е основа на нашата демокрация, защото без поверителност едни хора могат да използват властта, за да влияят на други. Този риск налага разпределеното съхраняване и оторизирания достъп като основни принципи на организацията и регламентирането на информационните процеси при е-управлението. Освен риска от неоторизиран достъп до информация така се избягва и ситуация, при която например държавен служител има достъп до всички данни за даден гражданин. Това често се основава на идеята, че информация, събрана за една цел, може да се използва за други цели. Възходът на технологиите за събиране, съхранение и обработка на големи масиви от данни и тенденцията към все по-широко използване на отворени системи правят по-лесно споделянето на информация. А това може да доведе и до по-целенасочено наблюдение и край на личната неприкосновеност.

Посоченият в началото на изследването и нееднократно изтъкван основен принцип на информационното общество, че достъпът до информация е основно човешко право, а информационните и комуникационните технологии създават предпоставки за свободното му упражняване, в крайна сметка недвусмислено означава, че глобалните информационни ресурси трябва да се използват при спазване на основните човешки и граждански права и свободи. В действителност, както вече отбелязахме, все повече се увеличават опитите за ограничаването им и за увеличаването на правомощията на държавата за навлизане в личния си живот.

В отговор на тенденциите за промяна в законодателството според приетите от Съвета за правата на човека и Глобалната мре-

жова инициатива водещи принципи за бизнес и човешки права още през 2011 г., технологичните компании трябваше убедително да покажат, че стоят зад своите потребители и се стремят да действат по-прозрачно. Глобалната мрежова инициатива е международна организация от компании, правозащитни организации, инвеститори и учени, които групово се изправят пред проблемите на корпоративната отговорност в технологичния сектор.

Ясно е, че развитието на технологиите ще продължи да увеличава възможностите за достъп до информация, а в същото време ще се увеличават предизвикателствата пред киберсигурността и опитите за нарушаване или ограничаване на неприкосновеността на личния живот, като „битката“ в това направление се очертава да бъде жестока и безкомпромисна.

Друг проблем, свързан с баланса между прозрачност и право на личен живот в контекста на развитието на „доброто управление“ и е-демокрацията, е свързан с различното отношение на поколенията по въпроса. Правото на неприкосновеност на личния живот е обект на промяна с течение на времето. Много често младите хора разкриват повече неща за живота си, отколкото възрастните хора (например във Фейсбук и други социални мрежи). Освен това индивидуалната представа за *лично* и *неприкосновено*, което всеки иска да запази, може да се променя в зависимост от контекста и момента във времето.

Тук ще маркираме още един въпрос, имащ отношение към темата – въпроса за държавните служители в качеството им на такива и в качеството им на граждани. Като граждани, те трябва да пазят неприкосновеността на личния си живот, освен когато това право подкопава колективната сигурност. В същото време не трябва по принцип да се допуска правителствата (като институции) да работят в тайна и трябва да се гарантира, че техните решения и действия са прозрачни и подлежащи на проверка. Една от отговорностите на политиците и държавните служители е да гарантират, че правителството работи по прозрачен начин, докато в същото време държавните служители поддържат неприкосновеността на личния живот като граждани. По-нататък ще разгледаме ограниченията на правото на достъп до информация, които са допустими и естествено обусловени, в контекста на други права или националната сигурност. Както прозрачността, така и неприкосновеността на лич-

ния живот са основни градивни елементи за гарантиране на демократично общество, които са пряко обвързани с правото на достъп до информация. Регламентирането на правото на информация в съвременната история се определя на международно ниво от множество актове, които често нямат задължителен характер при създаването си, но впоследствие стават основа, на която стъпва законодателството в различните държави.

За първи път за правото на човека да търси, получава и разпространява информация, се говори в чл. 19 на Всеобщата декларация за правата на човека на ООН от 1948 г.

С утвърждаването на позицията, че основните права на човека и тяхната сигурност са въпрос не само на вътрешното, но и на международното право, започва нов етап в общественото развитие. Идеята започва да се институционализира, създават се международни организации, чиято основна цел са поощряването и контролът върху спазването на закрепените в юридически задължителни актове основни права на човека. Създават се организации, общества, комитети, в рамките на които се разработват и приемат основни конвенции. Първите международни мерки за сигурност на правата на човека са свързани с премахването на робството, с хуманитарното право и др., но истинският разцвет идва със създаването на ООН през 1945 г. в Сан Франциско, САЩ. ООН е реакция на международната общност на последиците, предизвикани от Втората световна война, и е израз на стремежа да се предприемат адекватни мерки за повишаване на общата сигурност и спазване на правата на човека в света. В Устава на организацията изрично е посочено, че спазването и поощряването на правата на човека са важна цел за нея, и това превръща Устава не само в документ с организационно-устройствен характер, но и в документ с фундаментално значение.

През 1946 г. се създава Комисията по правата на човека на ООН, която и днес е основен орган на Организацията в тази материя. Във времето са били създадени различни подкомисии по отделни направления – като например тази за правата на малцинствата, която и сега продължава да формира политиката на ООН в областта на правата на човека. Веднага след създаването си Комисията започва подготовката на декларация (харта) по правата на човека.

Декларация за правата на човека няма за цел да обвърже държавите с юридически задължения, а по-скоро да определи целите,

за чието постигане те трябва да работят заедно. Особеното значение на Декларацията е, че тя е провъзгласена като общ стандарт, който да бъде постигнат от всички нации и народи. Юридическият ѝ статус е на резолюция без юридическа сила, но с огромно нравствено значение. В Декларацията са закрепени цялата палитра основни, фундаментални права и свободи, както и някои задължителни клаузи за подобен вид актове по това време. В този смисъл тя съдържа:

– клауза против дискриминацията;

– забрана на робството, крепостничеството и търговията с роби;

– забрана на изтезания, на жестоко и нечовешко унизително отнасяне;

– право на признаване на правосубектността на индивида;

– клауза за равенство пред закона;

– право на сигурност;

– забрана на произволните арести;

– право на справедлив съдебен процес;

– презумпция за невинност;

– неприкосновеност на личния живот;

– право на свободно придвижване;

– право на гражданство;

– право на собственост;

– свобода на мисълта, съвестта и религията;

– право да се търси, получава и разпространява информация;

– свобода на мирни събирания и сдружаване;

– право на труд;

– право на социална сигурност;

– право на образование;

– право на достойно жизнено равнище – право на социален и международен ред, при който правата и свободите да може да бъдат осъществени.

Освен правата тя включва и задължения, или т.нар. *ограничителна клауза*: при упражняването на своите права човек може да бъде подчинен на ограничения, установени със закон, с цел да се осигурят необходимото признаване и зачитане на правата и свободите на другите и удовлетворяването на справедливите изисквания на морала, обществения ред и общото благоденствие на всяко де-

мократично общество. Тъй като липсата на юридическа сила на Декларацията се оказва проблем, почти веднага след нейното разработване се преминава към подготовка и на юридически задължителни документи.

Редица други международни актове разглеждат правото на информация и посочват насоките за реализацията му като гаранция на развитието на устойчиво гражданско общество. Ще акцентираме върху някои от основните.

ЕВРОПЕЙСКА КОНВЕНЦИЯ ЗА ЗАЩИТА НА ПРАВАТА НА ЧОВЕКА И ОСНОВНИТЕ СВОБОДИ (1950). Правителствата, подписали тази Конвенция като членове на Съвета на Европа, се основават на Всеобщата декларация за правата на човека. Декларацията има за цел да осигури всеобщото и ефективно признаване и спазване на човешките права като основа на справедливостта и мира в целия свят. Тези права се смятат за фундамент на демокрацията и може да бъдат осъществени по-ефикасно само при признаване на върховенството на закона. В чл. 10 на Декларацията „Свобода на словото“ се определя правото на информация без намеса на властта и без определяне на граници. Декларацията определя и възможните ограничения на тези права и свободи.

ЙОХАНЕСБУРГСКИТЕ ПРИНЦИПИ „Национална сигурност, свобода на самоизразяването и достъп до информация“, приети през 1995 г. от група експерти по международно право, се основават на международни и национални закони и стандарти, отнасящи се до правата на човека. В документа се подчертава важността на свободата на изразяване и свободата на информация за прогресивното развитие на гражданското общество. Изрично се посочва, че за да бъде осъществяван контрол върху дейността и поведението на правителствата, „е наложително да има достъп до съхраняваната информация“. Регламентират се принципите, на които трябва да се основава всяко ограничение на достъпа до информация, засягащо националната сигурност.

ОКИНАВСКАТА ХАРТА НА ГЛОБАЛНОТО ИНФОРМАЦИОННО ОБЩЕСТВО (2000 г.) [45] формулира стратегията за развитие на човешката цивилизация през XXI век и определя информационните технологии като един от най-важните фактори, които подпомагат разширяването на свободния обмен на информация, който от своя страна стимулира устойчивото развитие в контекста

на основаната на знание глобална икономика. С други думи, наличието на надеждно осигурено право на информация в крайна сметка означава повишаване на темповете на икономическото развитие и съответно на жизнения стандарт на хората.

Признавайки огромната роля на информацията, лидерите на Г-8 обръщат внимание и на опасностите, които възникват в този нов свят.[1]

Първата от тях е несанкционираният достъп до информация. Поставен е въпросът за осигуряване на свободно от престъпления киберпространство.

Като втора сериозна заплаха е определено „дигиталното разделение" вътре във всяка държава и между отделните държави. Различията в икономическото развитие неминуемо водят до неравенство по отношение на достъпа до информационните мрежи, а значи – и до сериозно задълбочаване на пропастта между развитите и развиващите се страни и региони, между богатите и бедните слоеве на населението. В епохата, когато развитието на икономиката и промишлеността се определя от информацията и знанията, отсъствието на достъп до тях означава и отсъствие на възможности за развитие. Този, който не е включен в световната информационна мрежа, не е включен и в световния цивилизационен процес.

Тази печална закономерност се проявява и в личностен план. По тази причина в Окинавската харта се формулира необходимостта всеки човек да има достъп до информационните и комуникационните мрежи. Осигуряването на такъв достъп е възможно единствено чрез сътрудничество между управляващите, бизнеса и гражданските организации.

Разбира се, преодоляването на проблема с дигиталното неравенство има множество аспекти. Един от най-важните е **образованието**, или казано по друг начин, ИНФОРМАЦИОННАТА ГРАМОТНОСТ. За да може да използва информационните възможности на световната мрежа, човек трябва да знае как да се свърже и как да работи със съвременните технологии. Държавите членки на Г-8 си поставят задачата да предоставят на всички граждани възмож-

[1] Правителственият форум на група от осем водещи индустриални държави преди 24 март 2014 г. Към момента е във формат Г-7.

ност да усвоят и да получат навици за работа в киберпространството, като проявяват особена загриженост за тези граждани, които в противен случай не биха имали достъп до образование и професионална подготовка.

За трета сериозна заплаха се смята отсъствието (или недостатъчната разработеност) на единни правила, свързани с достъпа и използването на информация и технологии и с различията в усилията на отделните държави при формиране на такива единни правила.

ЮНЕСКО (Организацията на Обединените нации по въпросите на образованието, науката и културата) също приема ръководни принципи за развитие и съдействие на правителствената информация, явяваща се обществено достояние, 2004 г. (Policy Guidelines for the Development and Promotion of Governmental Public Domain Information). Целта на ръководните принципи, предложени от ЮНЕСКО, е да се установи база и да се определят принципи за разработка на информационна политика в областта на създаването, разпространението, съхранението и използването на информация, представляваща обществен интерес. Ръководството е насочено към:

- определяне на информацията за обществен достъп и изясняване на нейната роля и важност;
- формулиране на принципи, които да помогнат да се определят пътят на развитие на информационната политика, инфраструктурата и службите за осигуряване на достъп до информация, създавана от държавните органи и представляваща обществен интерес;
- подпомагане на създаването, архивирането и разпространението на електронна информация за обществен достъп и развитие, акцентиращо върху осигуряването на мултикултурно, многоезично съдържание;
- подпомагане на възможностите за достъп до информация на всички граждани, за тяхното индивидуално и обществено развитие, като се акцентира особено върху обществените групи, заплашени от изолация.

Най-пълно правото на достъп до информация, участието на обществеността в приемането на решения и достъп до правосъдие по въпросите на околната среда намира израз в ОРХУСКАТА КОНВЕНЦИЯ, която след доста преговори при широко международно

участие е подписана от представители на 40 европейски държави в Орхус (Дания) през 1998 г. Конвенцията е не само международно съглашение в сферата на опазването на околната среда, но и важен инструмент за развитие на демокрацията и правата на човека. Този нов вид международен договор установява не само взаимоотношенията и задълженията на страните като субект на международното право, но и вътрешните отношения на държавата с гражданите и обществеността, възлагайки на органите на управление задължения да приемат решения в условията на прозрачност, отчетност и открит достъп до информация с участието на обществеността в процеса и отчитайки нейното мнение.

Кръгът на субектите, свързани с правото на достъп до информация в съответствие с Орхуската конвенция, е достатъчно широк: това е обществеността, която съгласно документа означава едно или повече физически или юридически лица.

Важно е това, че запитването за информация може да бъде предявено от което и да е лице, без то да доказва своята лична заинтересованост от нея.

В Конвенцията се употребява терминът „заинтересована общественост", под който се разбира общественост, на която оказва или може да окаже влияние вземането на решения. Тези ограничения на кръга субекти не се отнасят до правото на получаване на информация. Доказването на заинтересованост е необходимо за привличане в процеса на вземане на решения и за обръщане към съд заради нарушени права. Неправителствените организации, които се занимават със сигурността на околната среда и отговарят на изискванията на националното законодателство, се смятат за заинтересовани.

Правото на човека на информираност кореспондира със задължения на държавните органи да предоставят информация във форма, в която тя е потърсена, в максимално кратки срокове, но не по-късно от един месец от датата на поискването ѝ. Ако официалният орган няма на разположение търсената информация, той е длъжен по най-бързия начин да уведоми заявителя към кой държавен орган е необходимо да се обърне, или да предаде въпроса към този орган, като информира за това заявителя.

Държавните органи са длъжни да имат на свое разпореждане информация за екологичната среда, която се отнася до тяхната

дейност, и постоянно да я обновяват. Те са задължени да осигурят безплатен достъп на обществеността до списъци, регистри или архиви, достъпни за нея, като постепенно увеличават обема на тази информация в електронните бази данни.

В Орхуската конвенция са определени възможностите за отказ да се предостави информация. Такива в частност са обстоятелствата, при които обнародването на определена информация може да повлияе на международните отношения, националната отбрана или безопасност. Също така са включени случаите, когато информацията засяга осъществяването на правосъдие или разследването на криминални дела. Преценката на основанията трябва да се тълкува, като се отчита заинтересоваността на обществеността от обнародването на информацията. В случаите, които представляват непосредствена заплаха за здравето на хората или околната среда, цялата информация, която би позволила на обществеността да предприеме мерки за предотвратяване или намаляване на вредата, трябва да бъде разпространявана веднага сред обществеността, която е потенциално заплашена.

Важно значение има и задължението на органите да привличат обществеността към процесите на вземане на решения по конкретни дейности, на по-ранен стадий да предоставят пълната информация за дейността, която планират, да организират публични прояви и изслушвания и да вземат под внимание общественото мнение.

Гаранция за реализацията на правата на достъп до информация и участие във вземането на решения е достъпът до правосъдие. Той определя принудителния характер на съблюдаването на екологичните права и осигуряването на реализация на постановките на Конвенцията, доколкото което и да е лице, смятащо, че неговите права на информация или вземане на решения, свързани с екологията, са нарушени, може да се обърне към съд за защита на законните си права и интереси.

Може да се каже, че Орхуската конвенция преследва глобални цели, доколкото засяга универсални права.

През 2006 г. Европейският парламент и Съветът на Европа

приемат ***РЕГЛАМЕНТ (ЕО) № 1367/2006[2] относно прилагането на разпоредбите на Орхуската конвенция за достъп до информация, публично участие в процеса на вземане на решения и достъп до правосъдие по въпроси на околната среда към институциите и органите на Общността.***

Целта на Регламента е създаване на правила за прилагане на Конвенцията, като са формулирани основните им опори:

„а) гарантиране на правото на публичен достъп до информация за околната среда, получена или изготвена от институции или органи на Общността, и с която те разполагат и чрез установяване на основните срокове и условия за, и практическото уреждане на изпълнението на това право;

б) гарантиране, че информацията за околната среда се предоставя непрекъснато и се разпространява на обществеността, с цел да се постигне възможно най-широката системна наличност и разпространение. За тази цел използването по-специално на компютърна телекомуникационна и/или електронна технология, когато е налична, следва да бъде насърчавано;

в) осигуряване на публично участие в планове и програми, свързани с околната среда;

г) предоставяне на достъп до правосъдие по екологични въпроси на нивото на Общността съгласно условията, определени в настоящия регламент“.

През 2008 г. бе приет първият в света правнозадължителен договор, гарантиращ достъпа до информация – ***Конвенцията за достъп до официални документи на Съвета на Европа (CETS № 205)[3]***.

Изработването на текста на Конвенцията за достъп до официални документи започва през януари 2006 г. и е съпроводено от широкомащабна кампания от страна на много граждански органи-

---

[2] Пълният текст на Регламента може да бъде намерен на следния адрес: http://www.aip-bg.org.

[3] Конвенцията е публикувана и в превод на български език с последна редакция от март 2016 г. от Програма достъп до информация: http://store.aip-bg.org/legislation/coe/conv_access_bg.pdf.

зации, 12 европейски информационни комисари, няколко правителства и др. Към текста на Конвенцията са направени препоръки относно стандартите за достъп до информация, които се залагат в нея, с цел повишена прозрачност. Независимо от широката подкрепа на тези препоръки те не са отразени в текста при приемането на Конвенцията. Конвенцията е отворена за подписване и към настоящия момент, като стремежът е да се създаде силен наблюдаващ орган, който да контролира прилагането ѝ.

Освен маркираните инициативи и актове с основно значение за реализацията на правото на информация, все повече се увеличава броят на държавите по света със специално законодателство или нормативни актове в тази област. Към м. май 2016 г. те са 106, по данни на Open Society Justice Initiative[4].

ДОСТЪП ДО ИНФОРМАЦИЯ – ТЕХНИЧЕСКИ, ЕТИЧЕСКИ, ОБРАЗОВАТЕЛНИ, ФИЗИЧЕСКИ И КУЛТУРНИ АСПЕКТИ

Както вече подчертахме, прозрачността има комплексен и многоаспектен характер, който е неразривно свързан с достъпа до информация. А той от своя страна може да бъде разглеждан от различни аспекти: технически, етически, образователни, физически и културни. Ще маркираме някои от основните характеристики на всеки от тях.

Използването на информационните и комуникационните технологии е едно от условията за реализация на достъпа до информация. Новите технологии все повече разширяват възможностите за достъп до информационни ресурси и създават условия за облекчаване на комуникацията между граждани и управленски органи. По този начин позволяват широко участие на всички заинтересовани страни в процеса на управление. Значението им за реализацията на личността – професионална, лична и обществена – е повод за множество изследвания. Социално-икономическото планиране и управление, производството и транспортът, банките и борсите, средствата за масова информация и издателствата, отбранителните системи, социалните и правоохранителните бази данни,

[4] Данните са публикувани на следния адрес: http://www.right2info.org/laws/constitutional-provisions-laws-and-regulations.

услугите и здравеопазването, образованието и учебните процеси, или казано накратко, всички сфери на живота, днес са немислими без информационните и комуникационните технологии.

Информатизацията на обществото доведе до коренни промени във всички обществени структури и процеси. Като термин „информатизация“ все още често се тълкува в контекста, в който преди се използваха термините „автоматизация“, „компютризация“, „електронизация“. Но информатизацията е не само нов способ за обозначаване на известни проблеми. Употребата на този термин се отнася до новото разбиране за значението и последствията на рязкото увеличаване на производителността на труда върху основата на новите информационни и комуникационни технологии.

Информатизацията на обществото може да бъде определена като организиран социално-икономически и научно-технически процес на създаване на оптимални условия за удовлетворяване на информационните потребности и реализацията на правата на гражданите, органите на държавната власт, организациите и обществените обединения, основан на формирането и използването на информационните ресурси. Според редица автори информатизацията включва три взаимносвързани процеса:

- медиатизация – процес на усъвършенстване на средствата на събиране, съхраняване и разпространяване на информацията;
- компютризация – процес на усъвършенстване на средствата за търсене и обработка на информацията;
- интелектуализация – процес на развитие на способности за възприемане и създаване на информация, т.е. повишаване на интелектуалния потенциал на обществото, включително чрез използването на средствата на изкуствения интелект.

Последователното и настойчиво изпълнение на тези три процеса води до радикални и революционни изменения на социалната структура.

Понятието „информатизация на обществото“ е с много по-широк смисъл от „компютризация на обществото“. При компютризацията основно внимание се отделя на развитието и внедряването на техническата база, осигуряваща оперативно получаване на резултати от обработката на информация и нейното натрупване.

При информатизацията обществото създава комплекс от мерки, насочени към осигуряване на пълното използване на достовер-

ни, изчерпателни и своевременни информация и знания за всички видове човешка дейност. По тази причина на информатизацията се гледа като на един по-сложен процес, насочен към бързото усвояване на информацията с цел удовлетворяване на потребностите.

Информатизацията е тясно свързана с процесите на взаимодействие на социалната интелектуализация, повишаването на творческия потенциал на личността и нейната информационна среда.

Съществуват два основни теоретико-методологични подхода към информатизацията на обществото:

• технократски, при който информационните технологии се смятат за средство за повишаване на производителността на труда и тяхното използване се ограничава основно в сферите на производство и управление;

• хуманитарен, при който информационните технологии се разглеждат като важна част от обществения живот, имаща значение не само за производството, но и за социалната сфера.

Концепцията за информатизация на обществото включва преди всичко създаването на унифицирани в широк спектър приложения и напълно структурирани информационни и комуникационни технологии, които обхващат процесите на събиране, натрупване, съхранение, търсене, обработка и предаване на цялата информация, необходима за дадена обществена дейност и за функциониране на обществото като цяло.

Информационната наситеност обаче не само промени света, а и създаде множество проблеми, които не бяха предвидени в прогнозите за развитие. Неумението да се оценява правилно информацията, стана причина за загуба на устойчивост. С нарастването и усложняването на системите възникнаха информационни бариери, които не можеше да бъдат преодолени без наличието на необходимите технологии. Например по данни от теоретичната и експерименталната психология човек не може да съпостави или сравни едновременно повече от 5 до 9 обекта. По тази причина може да се каже, че развитието на информационните технологии донякъде беше предопределено от развитието и усложняването на антропогенната част на света.

Често и днес с понятието „информационни технологии“ се визират програмните и електронните средства за събиране, съхраня-

ване, преработка, пренос и представяне на информация. Всъщност изброените информационни дейности са се извършвали много преди появата на компютрите и съвременните комуникационни средства. В това си качество информационните технологии се развиват в отговор на взривния информационен растеж на управляваните системи. В настоящия момент под „информационни технологии“ се разбират интегрирани съвкупности от научни, технологични и инженерни дейности, специализирано оборудване и специфични техники за управление, които се използват при създаването, обработката, съхраняването, разпространението и потреблението на информацията. С развитието им нараства и „прозрачността“ на света, а скоростта и обемът на предаване на информация се превръщат в още един фактор за световна интеграция. Тази интеграция може само да се приветства, ако нейно следствие не е размиването на регионалните и културно-историческите особености на развитието. Тоест задължително трябва да се отчита фактът, че информационните технологии включват както технически, така и социален аспект. От една страна, може да бъдат посочени различни примери за това как информацията, която трудно се анализира и оценява поради недостатъчно интелектуално осмисляне, се превръща в дестабилизиращ фактор за развитието. От друга страна, от социална гледна точка информационните технологии са тези, които направиха качествена промяна в масовите комуникационни системи. Тази промяна оказва съществено влияние върху всички обществено-икономически процеси. Появата на дестабилизираща информация е сигнал за разрива между наличието на информация и възможностите за нейната правилна оценка, сигнал за необходимост от ново интелектуално развитие в познанието за закономерностите на развитието. За съжаление, това развитие често е зависимо от различни ограничения: биологични, образователни, личностни, т.е. ограничения на интелектуалния ресурс, ограничения на скоростта на интелектуалното самопознание на обществото. По тези причини целта на развитието на съвременните информационни и комуникационни технологии трябва да е такава, че те да носят полза както за отделния човек, така и за обществото като цяло, а не да съдействат за оформянето на нов вид социално неравенство и да играят ролята на дестабилизиращ фактор.

Демократизацията на обществото, нарастването на информа-

ционната активност и потреблението станаха предпоставка за ново определение за същността на информационните технологии като средство за управление на общественото съзнание. Към тези средства се отнасят избирателните технологии, рекламните технологии, невронно-лингвистичното програмиране и други технологии в социалната сфера.

Рекламната и политическата информация в по-голямата си част се предоставят на потребителя „безплатно“. Разходите за тях се заплащат от заинтересованите от формирането на определени интереси или нужди. Потребителят заплаща впоследствие, при купуването на дадена стока, използването на услуга или съдействайки за реализирането на дадена рекламирана идея. Възможностите за манипулативно използване на информацията и технологиите за нейното управление и разпространение са един от проблемите, стоящи пред съвременната демокрация. Ако целите на управляващите и разпространителите на информация, от една страна, и на обществото, от друга, не съвпадат, се получава неизбежен информационен стрес у потребителите на информация заради неоправдани очаквания и криза на доверието в информацията; това също така е причина за затруднения в адаптацията на обществото към глобалните промени.

Възможностите за създаване на монопол върху информационните и комуникационните технологии, а по този начин – и върху информацията и нейната интерпретация, водят до засилване на „информационното затъмнение“ и нарушаване на демократичните права, а оттам – и до нарушаване на устойчивото обществено развитие.

Една от основните теми на редовно провежданите от Съвета на Европа конференции на министрите по очертаване на насоките на политиката и прилагането на актовете в областта на средствата за масова комуникация в европейски мащаб е преодоляването на различията в степента на развитие на отделните страни и неравностойното им участие в процеса на интеграция. Концентрирането на инвестиции за телекомуникационни услуги в развитите страни още повече задълбочава пропастта между тях и развиващите се страни. Появява се нова форма на бедност – информационна бедност, засягаща не само индивиди, слоеве от населението, но и цели държави.

Днес повечето специалисти предпочитат да използват понятието „информационна бедност“ пред „информационно неравенст-

во“. Много често и днес информационното неравенство се възприема само като отсъствие на физически достъп до информационна и комуникационна техника и технологии. Информационното неравенство всъщност включва ограничения от различен характер и е един от основните аспекти, свързани с възможностите и правата за достъп до информация.

Изследванията показват, че различните групи са свързани по различен начин в света на информационните и комуникационните технологии – от пълна интеграция до пълно отсъствие. Може да бъдат определени три основни групи от населението според използването на информационните и комуникационните технологии:

1. Такива, които използват информационни и комуникационни технологии. В тази група са включени всички, които осъзнават ролята на информацията, възползват се от възможностите и правото на информация и по този начин активно участват в изграждането на новата информационна среда.

2. Такива, които имат желание да ги използват, но по някаква причина (техническа, икономическа, образователна, здравословна или др.) не могат да се възползват от предимствата на информационните и комуникационните технологии. Това са хора, осъзнали значението на информацията, които при съответните условия биха се включили към групата на потребителите.

3. Такива, които не желаят да ги използват по каквато и да е причина. Тази група се състои от тези, за които всичко, свързано с информационните и комуникационните технологии, се намира извън техния интерес. Това са информационно пасивните хора, които са потенциално най-застрашени от социална дезинтеграция и изключване.

Социалният и етическият аспект на правото и на достъпа до информация включват и някои въпроси, които и досега са актуални и за които предстои да се търси правилното решение. Това са въпросите, свързани с ролята на притежателите на инфраструктурата, на производителите на програмни продукти, авторите, издателите, правителствените и международните организации за широкото разпространение на информацията сред тези слоеве от населението или в тези страни, където достъпът до информационните ресурси е недостатъчен.

Друг кръг от въпроси е свързан с баланса между свободната

или безплатната информация (разпространявана за широк кръг потребители от правителствени и международни организации) и интелектуалните информационни продукти, осигуряващи ефективен достъп до знание и възможност за вземане на ефективни решения.

Решаването на тези и други проблеми е пряко обвързано с участието на специалисти от различни области, като при това се отчита важността на пълноценното обществено участие във формирането на политики и решения. Тук изпъква една от характеристиките на информационното общество – като общество с развита сфера на услугите, в което се признава важната роля на образованието и науката, на знанието, на получаването и разпространението на информация.

С цел справяне с тези проблеми се наложи разширяване на концепциите за „универсалната услуга“ и „универсалния достъп“ до информация по отношение на новите информационни и комуникационни услуги, прилагани до този момент в далекосъобщенията и телекомуникационния сектор. В „Зелена книга за либерализацията на телекомуникационната инфраструктура и мрежите за кабелна телевизия“ (1994)[5] универсалната услуга се дефинира като *„достъп за всички потребители до даден минимум от услуги с определено качество на приемлива цена, въз основа на принципите на всеобщност, равенство и непрекъснатост“*. Поради скоростта на развитие на технологичните процеси и нарастването на комплектността на услугите дефиницията на универсалната услуга трябва да се изменя динамично, за да може да отразява тези процеси. Универсалната услуга е свързана с предоставянето на всички потребители на телефонни услуги, на интерактивни и онлайн информационни услуги, като ползване на глобалната информационна мрежа интернет, достъп до бази данни, електронен обмен на информация, съобщения и др.

Универсалният достъп до информация е задължително условие за съществуването на информационно общество и предпоставка за пълноценното участие на гражданите в демократичните институции. Той е гаранция за правото на всеки човек да търси, полу-

[5] http://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32002L0022

чава и разпространява информация независимо от националните граници. Универсалният достъп включва достъп до информационните супермагистрали, до телекомуникационни услуги за училища, университети, библиотеки и други културни институции, които са фундаментът на информационното общество.

Етическите аспекти на достъпа до информация са свързани с едно сравнително ново поле на етиката, обусловено от развитието на информационните технологии и произтичащите от това промени в съвременните общества като цяло, както и във формите на човешкото общуване. Тези проблеми, които са обект на изследване в различни науки, днес често попадат в обсега на формиращото се поле на т.нар. информационна етика като приложно поле на етиката.

В западната традиция информационната етика има своите основи още в устната култура на атинската демокрация и до началото на XX век се характеризира с две основни идеи – свобода на изразяването и свобода на печата и пресата. Третият елемент, появил се в наше време, във времето на мрежовото общество и електронната информация, се нарича свобода на достъпа и право на комуникация.

Етическите въпроси, свързани с информационния достъп, резултират в проблемите на публичния достъп до информация и услуги, както и в човешките права на комуникация. Въпросите за достъпа може да се разглеждат като индивидуални и социални.

Индивидите и групите са заинтересовани от свободния и неограничен достъп до информация и свободната комуникация (един към един, един към много, много към един, много към много). От етическа гледна точка достъпът до информация и средства за комуникация може да се разглежда както като право на всеки човек, така и като свързан с правото на личен живот и неприкосновеността на личните данни, от гледна точка на авторските права и т.н. Тези права и рисковете при тяхната реализация бяха засегнати в различна степен в предходните раздели. Тук ще представим още един аспект, свързан с риска за обществото от гледна точка на възможностите да се манипулира общественото мнение чрез манипулация на медиите. В контекста на е-демокрацията осигуряването на различни канали за достъп и комуникация между управлението и обществото е от първостепенно значение.

Един от основните канали за формиране на обществено мнение в настоящия етап на развитие на демократичните общества ес-

тествено са медиите, независимо от техния вид. Използването на медийното пространство за създаване на обществени нагласи не е феномен на съвременното общество. Според Ноам Чомски съществуват две концепции за демокрация. Едната твърди, че демократично е онова общество, в което хората имат възможността да участват по някакъв смислен начин в управлението на собствените си дела и където средствата за информация са достъпни и свободни.

Другата концепция подкрепя тезата за „демокрация на зрителите", при която малка група управляващ елит определя дневния ред и мисленето на обществото, „а средствата за информация трябва да са с ограничен достъп и под строг контрол". Според автора тази концепция има дълга история, още от ранните демократични революции в Англия от XVII век, когато широко са проповядвали този възглед. Развитието на тази идея и проблемът за медиите и дезинформацията са основни според Чомски в американския модел на демокрация. В демократичното общество проблемите за независимостта на медиите, обществените им функции и медийната етика са обект на множество изследвания. Така наречената *демократична цензура* се свързва с изопаченото поднасяне на информация и огромния поток от интерпретации и детайли. В случая няма класическа форма на цензура, каквато е позната при авторитарни и тоталитарни системи, т.е. няма забрана на информация, а по-скоро контрол или принуда към конюнктурно мнение чрез селекция или нихилизъм. Невъзможността да се обхване предложеното свръхколичество информация, често води до загуба на интерес или директно приемане на наложените мнения и идеи.

Физическият аспект на достъпа до информация може да бъде разглеждан като възможност за използване на информация от всеки, дори от хора с различна степен на увреждания. Във всяко отношение прилагането на нови и стари технологии би могло да намали значително действието на някои от тези бариери.

Културни особености могат да ограничат достъпа до информация на определени социални групи или да направят невъзможно изразяването на тяхната гледна точка по много въпроси. Новите технологии създават нови информационни общности, но могат и да направят културните бариери много по-здрави.

Широкият спектър от въпроси, свързани с моралните и етическите аспекти на свободата на изразяване на мнение и свободата на

информацията, се отнасят до дискусията за публичната сфера. Публичната сфера в контекста на теорията на Хабермас съществува само там, където всеки гражданин има равно право и възможности за достъп и участие в диалог, дискусия, дебат. Така частните индивиди се превръщат в публика, която по този начин формулира мнение по един или друг проблем. Липсата на възможност за диалог и дискусия, дори при наличието на средства и възможности за изразяване на мнения по един или друг публичен проблем, всъщност означава наличие само на публично пространство. Основавайки се на теорията на Хабермас, Христо Проданов подчертава, че „комерсиализираните средства за масова информация превръщат публичната сфера в пространство, в което на преден план излизат рекламата и пиарът, свързани с комерсиални интереси, а не с рационалния и демократичен публичен дискурс“. При липсата на „чувствителност“ от страна на обществото към начина на работа на медиите, а именно информирането и изразяването на мнение да се съобразяват с две основни положения – истината и достойнството на човека, балансът на употребата на основните свободи не може да бъде гарантиран.

Не по-малко значение имат организационните аспекти. Организирането на информацията е основен елемент на достъпа до информация. Наложително е печатните и електронните източници да бъдат организирани по такъв начин, че да бъдат лесни за откриване, използване и разбиране от потребителя.

Не на последно място са образователните аспекти. Образованието, и то през целия живот, в наше време е задължително условие за реализация на гражданите в демократичното информационно общество. За да бъде то възможно, е необходимо да се осигури достъп до информация, независимо в какъв вид и на какъв носител е тя. От друга страна, образованият човек в мрежовото общество се нуждае от достатъчно високо ниво на информационна грамотност, така че да търси, намира, интерпретира, използва и разпространява информация и знания.

Анализът на различните аспекти на достъпа до информация ни дава основание да направим обобщението, че те са взаимносвързани, взаимнозависими и трябва да бъдат разглеждани като едно цяло с цел реализиране на основните човешки и граждански права и в крайна сметка – реализиране на действаща демокрация.

Е-УПРАВЛЕНИЕ И ДОСТЪП ДО ИНФОРМАЦИЯ. ПОЛИТИКИ НА ДЪРЖАВАТА ЗА ОСИГУРЯВАНЕ НА ДОСТЪП ДО ОБЩЕСТВЕНО ЗНАЧИМА ИНФОРМАЦИЯ

От маркираните дотук въпроси, свързани с достъпа до информация като изконно човешко право, можем да заключим, че освен конституционните и законовите основи от огромно значение са неотменимите му морални характеристики. Само наличието на определена информация и на определени знания някъде във виртуалната или реалната информационна среда не е достатъчно условие, за да се осъществи ефективен управленски процес (без значение дали управленският процес е конвенционален (традиционен), или управлението е електронно). За всички участници в този процес трябва да е осигурен достъп както до съхранената информация, така и до съхранените знания, които са релевантни на целта на съответното управление.

В този раздел се дефинират изследователски задачи, които разкриват връзката между е-управлението и механизмите за информационен достъп. Специално внимание е отделено на въпросите, свързани с достъпа до знания, както и на тяхното управление. Анализирани са възможните политики на държавата за осигуряване на достъп до обществено значима информация, като специално внимание е отделено на проблемите на сигурността като фактор за т.нар. информационна редукция.

СВОБОДА НА ИНФОРМАЦИЯТА И ДОСТЪП ДО ПРАВИТЕЛСТВЕНИ ДОКУМЕНТИ В КОНТЕКСТА НА КОНЦЕПЦИЯТА ЗА ПРОЗРАЧНО УПРАВЛЕНИЕ

Достъп до информация е практически необходим на всички стадии от живота на човека, за да се възползва от своите права – при получаване на образование, за да се устрои на работа, да получи достъп до програми за помощи на нуждаещите се, да построи или купи дом, да стартира частен бизнес или да получи пенсия. Без необходимата информация и лесен достъп до нея се създават предпоставки за корупция и измами. По тази причина всеки гражданин се нуждае от достъп до обществена информация, за да се довери на институциите и да е уверен в това, че те работят, както е необходи-

мо. Политиката и практиката на прозрачност са тези, които създават сами по себе си увереност в правилната работа на администрациите. В същото време информацията, която ни е нужна, може лесно да се „разтвори“ в лавината от ненужна информация. Самото наличие на информация е достатъчно условие, ако има условия за „информационно затъмнение“, т.е. ако липсва достъп до нея, ако информацията, която се получава, не е съдържателна, ако човек се сблъсква просто с огромно количество непроверени данни. Нещо повече, както нееднократно беше подчертавано, за реализирането на е-управление необходимо и задължително условие е гражданите да имат, от една страна, достъп до информация и данни за работата на управленските и административните органи. От друга страна – да са сигурни, че предоставяйки лична информация и комуникирайки си с тези органи по електронен път, те са максимално защитени.

Осигуряването на достъп до документи и информация на управленските и административните органи е едно от основните изисквания към съвременните правителства. Достъпът до информация съдейства на обществото за получаването на знание по различни въпроси и за обсъждането на множество проблеми. Достъпът дава сигурност срещу злоупотреби, лошо управление и корупция. Достъпът до информация служи и на управляващите да осигурят прозрачност и откритост на процесите на вземане на решения и по този начин да повишат доверието на гражданите към дейността на правителството и да съхранят гражданското демократично общество.

Основно изискване към управлението в съвременните демократични общества е да осигури система за широко предоставяне на информация за своята дейност. За целта се приемат закони, регламентиращи правата на гражданите и задълженията на администрацията за предоставяне на обществено значима информация. В предишния раздел споменахме, че в света над 100 страни са приели подробни нормативни актове, разглеждащи и регламентиращи свободата на информацията и достъпа до документи на правителствените органи.

Фактът, че повече от половината закони са приети през последните години, говори за повишената прозрачност на дейността на правителствата в отговор на нарасналите нужди на граждански-

те обществени организации, системите за масова информация и международните кредитори. Освен това много страни приемат и други закони, осигуряващи ограничения на достъпа до лични данни и позволяващи на физически лица да имат достъп до информация за себе си, която е под разпореждане на органите на властта и частните организации, а също така достъп до информация за околната среда и друга обществено значима информация.

Факторите, които оказват влияние върху приемането на закони, свързани със свободата на информацията, може да бъдат разделени на вътрешни и външни. В повечето страни гражданските организации, занимаващи се със сигурността при опазването на околната среда, и масмедиите играят немалка роля и съдействат за приемането на такива закони. В края на краищата самите правителства в много от тези страни признават необходимостта свободата на информацията да съответства на новите изисквания на времето и развитието на демокрацията.

Международни фактори. Органи, изиграли особено важна роля за приемането на закони за достъпа до информация, са:

• Съветът на Европа и Организацията на държавите от Американския континент – разработват ръководство за приемане на закони и модели за законодателство за свободата на информацията. През септември 2003 г. Съветът на Европа прие решение да разработи първата международна спогодба, свързана с достъпа до информация.

• Световната банка и Международният валутен фонд оказват влияние върху страните за приемане на законодателство за достъпа до информация с цел намаляване на корупцията.

• Организацията на обединените нации (ООН) изработва и приема разгледаната в предишния раздел Орхуска конвенция за достъп до информация за околната среда. С подписването на Конвенцията много страни се задължават да приемат национални закони, регламентиращи достъпа до информация за околната среда.

Модернизация и информационно общество. Широкото използване на интернет увеличава необходимостта от създаване на система и модернизиране на начините за предоставяне на информация от органите на управление. Разработката и внедряването на стратегии за електронно управление и електронно правителство изискват ясна регламентация на достъпа до информация.

Конституционни права. Преходът към демократично управление в повечето страни води до осъзнаване, че информацията е основно човешко право. Почти всички новосъздадени или модернизирани конституции включват правото на достъп до информация от официалните институции. Много често конституциите съдържат и особени условия за реализация на правото на достъп до информация за околната среда и правото на гражданите да получават достъп до информация за самите себе си.

Корупция и скандали. Липсата на прозрачност често води до възникване на кризи в различни сфери на обществения живот. За предотвратяването на подобни ситуации се провеждат редица антикорупционни кампании, които имат голямо значение за страните в преход, опитващи се да променят културата си на прозрачност и управление. В страни с утвърдена демокрация тези закони са приети вследствие на дълга кампания и натиск от страна на гражданското общество и множество политически скандали, свързани със здравеопазването и сигурността на околната среда. С увеличаването на възможностите за достъп до информация и разширяването на прозрачността става възможен постоянният контрол върху представителите на избирателната власт. По тази причина от 90-те години насам рязко се увеличават и случаите на обвинени в корупция политици или служители на държавната администрация. Тези тенденции дават основание да се говори за развитието на полупряка демокрация, т.е. контролът върху властовите институции може да бъде упражняван всекидневно. Погледнато в ретроспективен план, до 90-те години на XX век почти цялата дейност на парламентите и правителствата е свързана с информация, която се разпространява на хартиен носител, липсват общ език и формат, чрез които това да става електронно. Първите парламентарни сайтове се появяват в средата на 90-те години на XX век и чрез тях гражданите от всяка точка на света могат да получават по всяко време информация за парламентарната дейност. Днес немалка част от тези сайтове предоставят подробна информация за дейността на парламента, онлайн излъчване на заседанията и възможност за обществена дискусия и пряка връзка с парламентарните представители.

Общите черти и развитието на законодателството за свободата на информацията може да бъдат синтезирани в няколко аспекта. Фактът, че повечето закони, които регулират свободния достъп до

информация, са с множество общи черти, се основава отчасти на това, че законите, приети по-рано от някои страни, стават основа за изработване на останалите. Законът за свободата на информацията на САЩ, законите на Австралия и Канада – както национални, така и местни, са сред най-популярните и превърнали се в база и пример за добро законодателство в областта.

Най-общо може да се каже, че развитието на законодателството за свободата и достъпа до информацията е свързано с възможността на физическите лица да изискват и получават материали, намиращи се под разпореждане на органите на властта и различни държавни институции, от една страна, и от друга – с налагането на все по-голяма прозрачност чрез проактивно публикуване, т.е. предоставяне на информация, без да бъде изрично поискана. Трябва да подчертаем, че понятията „материали", „документи" или „информация" в този случай се тълкуват различно. Друг общ аспект е насочен към уеднаквяване на определенията (често се използват тези за материали, документи, информация) и разбирането за същността на понятието „обществена информация". Тези определения се различават едно от друго и в много закони през последните години бяха внесени изменения, за да се постигнат уеднаквяване и преодоляване на различията. Новите закони за достъпа до информация дават широка трактовка на понятието с цел различията да бъдат сведени до минимум. В това отношение един от най-напредничавите, още при създаването си, е Законът за достъп до обществена информация в Република България, който регламентира правото на достъп независимо от формата и носителя на информацията. Друг пример в това отношение е замяната в много от законите на понятието „документални файлови системи" с „компютърни".

За е-управлението ключови елементи при формирането на политика за осигуряване на гражданите с обществено значима информация са както определянето на съдържанието на понятието „обществено значима информация" и разширяването на сферата на достъпа до нея, така и разработването на концепция за управление и разпространение на обществени информационни ресурси.

Правилата за работа с документи и документални системи и достъпът до тях на външни потребители имат дългогодишна традиция и както вече беше посочено – правна регламентация в пове-

чето европейски държави. Възприет е принципът, че всяка демократична система изисква гражданите да са информирани за дейността и задачите на институциите като необходима предпоставка за активното им участие в обществения живот и управлението. Този принцип предполага необходимостта да се осигурят различни канали за достъп до огромната по обем информация, която е под разпореждане на различните административни органи. В повечето законодателни актове са регламентирани и ограниченията и изключенията при предоставянето ѝ, които са съобразени със сигурността на законните обществени и частни интереси, като се подчертава, че тези изключения не се влияят от вида на носителя на информацията.

Изграждането на политика и система за осигуряване на достъп до обществена информация започва с регламентирането на съдържанието на правото на достъп, като се определят:

- понятието „обществена информация“;
- субектите, задължени да предоставят достъп;
- видовете обществена информация, която субектите са задължени да предоставят;
- формите на достъп до информацията, предоставяна от задължените субекти;
- ограниченията за предоставяне на достъп до обществена информация;
- сигурност на правото на достъп до обществена информация.

За създаване на правилата за достъп на гражданите до информация на официалните административни и управленски органи в държавата е необходимо дадената информация да бъде отнесена към един от двата правни режима:

- информация с ограничен достъп;
- информация с открит достъп.

Трябва да се има предвид, че когато се говори за законни обществени интереси, се разбира запазването на националната сигурност, обществената безопасност и ред, предотвратяването на престъпления, икономическото благоденствие на страната като цяло.

Сигурността на личните данни цели да се запазят правата, доброто име и репутацията на частни лица, които се явяват „трета страна“ в отношенията *„администрация – съхранявана информа-*

ция – лица, желаещи достъп до информация“. Под „лични данни“ се има предвид всяка информация, свързана с идентифицирано или неидентифицирано лице. В много страни гласът и образът на частно лице се смятат за лични данни и са защитени от закона. Много често се използва и друга категория данни на особен режим както за придобиване, така и за съхранение и разпространение. Такива са например сведенията, разкриващи расов произход, политически мнения, религиозни или други вярвания, както и свързани със здравословното състояние и сексуалния живот.

Органите, които въз основа на закона са задължени да предоставят информация, като правило в законите са регламентирани като ***всички държавни органи***. В зависимост от типа на информацията към тях се включват и органите на местното и регионалното управление. В някои страни органите на законодателната власт, разузнавателните служби и службите за сигурност са изключени от списъка на задължените да предоставят информация. В някои страни се наблюдава и тенденция да се включват и неправителствените организации, особено тези, които получават финансови средства за реализация на обществени проекти. Често в списъка са включени организации като болници, а също така частни компании.

Ограничения в достъпа и надзор върху спазването на правото на информация. Естествено, в повечето закони са регламентирани общи изключения, забраняващи предоставянето на определени категории информация. Тези категории включват информацията, отнасяща се до националната сигурност, сигурността на личните данни и правото на личен живот, служебната тайна, търговската тайна и нелоялната конкуренция, осигуряването на обществения ред и др. Среща се и тенденция документите, решенията и материалите от заседанията на правителството също да бъдат включени в списъка с информация с ограничен достъп. Друга особеност в някои от законодателствата е свързана с установяването на значимостта на достъпа до информация. В такива закони се предвижда изискване за проверка на обществения интерес като отделен етап при разглеждането на искания за достъп до обществена информация. Дефинициите на понятието „обществен интерес“ често съдържат тавтологични определения, без да изясняват съдържанието.

Съществуват и различни механизми, процедури и схеми за контрол върху спазването на правото на информация и за обжалване на отказа за предоставяне ѝ. Те са административни процедури за оспорване на решения, съдебно оспорване и контрол, осъществяван от независими органи. Първият етап в повечето страни е вътрешното преразглеждане на дадено решение за отказ, като жалбата се подава към по-висшестоящо звено в организацията, където е подадено искането за достъп. Следващият етап от процедурата е обръщане към независим орган, като в много страни това е омбудсманът, който не може да издава решения със задължителен характер, но в повечето страни има достатъчно влияние за въздействие с цел преразглеждане на решенията.

В някои държави са създадени и независими информационни комисии като част от структурата на парламента. В други случаи комисиите са ангажирани както със свободата на информацията, така и със сигурността на личните данни или са свързани с надзорните органи. В трети случаи са сформирани специални експертни групи за преразглеждане на решенията по предоставяне на информация по запитване.

Крайна стъпка във възможностите за обжалване на отказа в повечето страни е съдебното обжалване. Често обаче тази стъпка представлява затруднение за гражданите, тъй като там, където съдът работи като външен, независим орган на властта, са необходими финансови средства и време за вземане на решение.

Докладът за състоянието на достъпа до информация в света през 2006 г., изготвен от Дейвид Банисар, съдържа обстоен анализ на състоянието на свободата на информацията в страните, създали законодателна база и регламентирали правото на достъп до информация. Независимо от констатацията, че през последните години е постигнат голям напредък в това отношение, се отчита, че все още може да се направи много за създаването на действително „прозрачно“ управление. Все още в много страни съществува доста широка „култура на секретност“ и тепърва е необходимо да се работи в посока на създаване на „култура на прозрачност“. Много от законите не отговарят на нуждите на дадената държава и само техните заглавия се отнасят до свободата на информацията. Десет години след публикуването на този доклад, независимо от тенденцията към налагане на все по-голяма прозрачност, можем да кажем, че направените констатации все още са

валидни. Това твърдение се обуславя от факта, че динамичните обществени и технологични промени налагат непрекъсната актуализация на законодателната база, а много често законите не се променят в зависимост от новите условия, произтичащи от измененията в обществото и технологиите.

Не по-малко са случаите, при които се приемат промени в законодателството, водещи до ограничения на достъпа до информация.

Съществува и още една тенденция на ограничаване на правото на информация – приемането на закони, свързани с борбата с тероризма. Към настоящия момент това е особено актуален въпрос, който е подложен на обществена дискусия в немалко държави. Приемането на такива закони неминуемо води до възможност да се ограничават основни права и свободи, и по тази причина обикновено е съпътствано от сериозна съпротива в демократичните общества. Често тази съпротива води до изменения на подобно законодателство след приемането му с цел възстановяване на баланса между свобода и сигурност. Като пример може да се посочи определянето на строги правила в какви случаи са допустими ограничения на правото на личен живот. Често в страни, създали първите законодателни актове за свободата на информацията, свободата на словото и правото на самоизразяване (Великобритания, САЩ), обществото приема доста равнодушно ограничаването на правата и свободите, наложено със законодателството, третиращо борбата с тероризма. За съжаление, събитията от последните години ни дават основание да заключим, че наличието на специално законодателство не води до сериозен успех в борбата с тероризма.

Ако се върнем към цитираното изследване на Банисар, ще видим, че и към момента законодателството, свързано с достъпа до информация, продължава активно да се развива и обогатява. В изследването се подчертава, че значително е нараснал броят на страните, които признават значението на достъпа до информация като основно човешко право и като важно условие за осигуряване на добро управление, както и за борба с корупцията. Към пролетта на 2006 г. 80 страни са закрепили като конституционно положение правото на достъп до информация. Около 70 страни са приели национални закони за свободата на информацията, а около 50 страни предприемат такива мерки. За 20 години до 2006 г. както конституции на страните от Централна и Източна Европа и Латинска Америка, така и конституциите на страни като Финландия и Норвегия включват правото на достъп до информация.

Тези права дават право на всеки гражданин или човек да търси информация от правителствените органи. Изследването показва, че конституцията на ЮАР предоставя най-широки права. В други страни, например от Латинска Америка, са дадени права само до личната информация за себе си. В трети страни се регламентира правото на достъп до информация за околната среда или информация, отнасяща се до личните права и интереси. В страни като Индия, Япония, Корея, Франция, Израел и Пакистан достъпът до информация, съдържащ се в конституциите, е компонент от свободата на словото и свободата на самоизразяване. Регламентирането на правото на достъп до информация в конституциите в някои страни е обвързано и с изискването да се създаде специален закон. Почти половината от държавите с конституционно установено право са разработили и национален закон за свободата на информацията. Някои от тези закони имат сами по себе си ниво на конституционно право. В Швеция законът „За свободата на пресата" е един от четирите основни закона, които образуват конституцията на държавата. В Канада и Нова Зеландия съдът определя значението на тези закони и конституционния им статус.

Тенденцията да се приемат закони за свободата на информацията, започва от северноевропейските страни и впоследствие обхваща не само Европа, но и целия свят. Много от страните в Западна Европа са приели подобни закони. Измененията в Централна и Източна Европа поставят началото на приемането на съответни закони, което започва от Украйна и Унгария през 1992 г. и завършва с Македония през 2006 г. За съжаление, съществуват и държави, за чиито закони се смята, че не функционират особено добре (Гърция, Италия, Испания).

Не по-малко са и държавите на Американския континент с вече установено законодателство в тази област. Актове, регламентиращи частично право на информация, са издадени в Аржентина, Боливия и Гватемала. Мексико заема лидерска позиция, тъй като има един от най-силните закони, като надзор над изпълнението му се осъществява от комисия по информацията и съвременна информационна система, които следят за регистрирането на всички запитвания и получаването на навременни отговори.

Тъй като законите на САЩ и Канада са доста остарели, е необходимо значителното им обновяване, за да отговарят на съвременните условия.

В азиатско-тихоокеанския регион темповете на приемане на

подобни закони са сравнително по-бавни. Правна регламентация на свободата на информация и достъпа до официални документи има в Австралия, Нова Зеландия, Южна Корея, Тайланд. Ефективността на тези закони обаче за последните години не се смята за достатъчна. В Япония освен национален закон има приети в над 3000 местни общини техни закони. В Индия през 2005 г. е приет нов закон, който освен всичко останало регламентира и създаването на комисия по информацията. В част от страните на Централна Азия се разработват законопроекти, но регламентацията на правото на информация все още остава в необозримото бъдеще. Почти същата е ситуацията на Африканския континент. Публикуваната от Банисар през 2015 г. актуализирана карта показва тенденция към разширяване на законодателството в посочените региони.

Обобщавайки развитието на законодателството, свързано с правото на информация, може да а направим заключението, че правната рамка е начална стъпка, която невинаги означава качество на изпълнение или прилагане. В някои случаи управлението в страните с относително слаби закони може да е много по-открито поради положителните усилия за спазване на законодателството и стремежа към прозрачност. В други случаи дори относително силни закони не могат да гарантират откритост, ако не се прилагат правилно. Независимо от тези разлики, с течение на времето по-силното законодателство за достъп до информация може да допринесе за постигането на напредък и насърчаването на правото на достъп до информация. Също така е важно да се отбележи, че макар откритостта да зависи и от фактори извън правната рамка за достъп до информация, силната правна рамка е важна предпоставка за пълното прилагане на правото на информация. Като пример може да се посочи изследването на качеството на законодателството за достъп до информация в света според 61 показателя, което към настоящия момент поставя Сърбия на първо място, докато Австрия остава в дъното на таблицата.[6]

---

[6] Рейтингът на правото на информация е програма, основана от Access Info Europe (OBOC) и Центъра по право и демокрация (CLD). Основната идея е да се предостави надежден инструмент за сравнително оценяване на цялостната правна рамка за достъпа до информация, като се посочват силните и слабите ѝ страни и по този начин се осигурява възможност за прецизиране на областите, нуждаещи се от подобрение. Адрес за достъп: http://www.rti-rating.org/.

Обща черта на повечето закони за свободата на информацията е задължението на правителствените органи редовно да публикуват определени категории информация, отнасяща се до структурата на правителството, висшите длъжностни лица, текстовете на законите и другите нормативни актове, информация за предложенията, подлежащи на разглеждане, информация за стратегиите в различни области и не на последно място – различни формуляри и бланки. Често в тези закони се регламентират и категориите информация, които не подлежат на обществен достъп по различни причини.

Изискването за активно публикуване на информация носи полза не само за гражданите, но и за повишаване на ефективността на работа на административните структури.

Още една тенденция в сферата на достъп до информация е нарастването на броя на използваните електронни системи за регистрация на запитвания и предоставяне на информация. Много от законите за свободата на информация изискват определени категории информация да се публикуват на уебсайтовете на администрацията, като с течение на времето тенденцията е тези категории да разширяват своя обхват. Гражданите, търсещи информация, получават все по-широки възможности да подават запитвания чрез електронна поща или електронни форми, поместени на сайта на дадената институция.

ИНФОРМАЦИЯ. ИНФОРМАЦИОННА СРЕДА – БАЗОВА КОНЦЕПЦИЯ. РАЗВИТИЕ НА СРЕДА ЗА ИНФОРМИРАНЕ

ИНФОРМАЦИЯ

Теории за информацията. Исторически бележки

В специализираната литература често се цитира една мисъл на великия Алберт Айнщайн, която в леко модифициран вид изглежда по следния начин: „АКО ЕДНА МАТЕРИАЛНА ИЛИ НЕМАТЕРИАЛНА СЪЩНОСТ НЕ МОЖЕ ДА СЕ ИЗМЕРИ, ТО ТЯ НЕ СЪЩЕСТВУВА“.

Не се знае дали тази прозорлива мисъл на Айнщайн е подтикнала младия учен и изследовател Клод Шенън да разработи съвременната Теория на информацията, но при всички случаи той дефинира понятието за количество информация и предлага мерки за нейното измерване. Тоест от този момент нататък (и според Айнщайн) информацията съществува и може да се използва като обективна реалност.

За основоположник на **Теорията на информацията** се смята американският учен Клод Шенън. През 1948 г. той публикува своя научен труд „Математическа теория на връзките (комуникациите)“. Там той блестящо защитава своите идеи за информацията, като я представя като феномен на нематериална субстанция и като средство за редуциране и управление на несигурността. Информацията в този контекст включва всички видове съобщения. Шенън предлага информацията да се измерва в математическия смисъл на това понятие, свеждайки я към избора между две значения, или двоични разреди – „да“ или „не“ („пълно“ или „празно“), полагайки по такъв начин основите на съвременната изчислителна математика и на теорията на комуникациите.

Обективната необходимост от измерване на информацията

дава основание на Шенън да дефинира понятието за количество информация в дадено съобщение като разлика в степените на несигурност преди и след получаването на това информационно съобщение.

Формулата на Шенън за изчисляване на количеството информация е следната:

$$i = -m\sum_{i=1}^{n} Pi.\log_2 Pi\,.$$

Според Клод Шенън основните направления в Теорията на информацията са в рамките на т.нар.:

• Апостериорна информация – информация, която е получена, известна, налична (т.е. тя съществува преди въвеждането на съответния експеримент/наблюдение/опит);

• Априорна информация – информация, получена в резултат на провеждането на определен експеримент. В зависимост от това какво е структурирано в нея, информацията може да бъде квалифицирана в няколко групи:

– **Събитие** – първичен, неделим елемент от представянето на информацията. Такива форми се явяват 1;0; потвърждение; отрицание; наличие; нищо; нещо, което не може да се раздели на помалки части;

– **Величина** – съвкупност от събития, подредени в едно определено измерение. Величината приема определен набор от събития и тогава имаме т.нар. дискретни величини. Когато величината приема допълнителен брой събития, се приема да бъде непрекъсната;

– **Функция** – представлява взаимовръзка между две величини, между величина и време, величина и пространство. В зависимост от типа на аргумента функциите биват дискретни и непрекъснати.

Множеството определения на термина „информация“, макар и интерпретирани по различен начин, дават основните инвариантни характеристики, които едно явление (състояние) трябва да притежава, за да го наречем „информация“. Сред съвкупността от източници тук ще цитираме Webster's Encyclopedic Unabridged Dictionary, 1989, с. 730, според който **информация е**: *„1. knowledge communicated or received concerning a particular fact or circumstance, news, ... 2. any knowledge gained through communication... 3. the act or*

fact of informing...“. Тази дефиниция определя ключовите думи „знание“, „комуникация“, „информиране“, които характеризират феномена „информация“.

Други такива, български, източници са:

Милев, Александър, Божил **Николов**, Йордан **Братков**. Речник на чуждите думи в българския език. 5. доп. и прераб. изд. София: Наука и изкуство, 2003. 904 с. На с. 313 е дадено значението на „информация“: **Информация** (от лат. informo „изобразявам“, „формирам“): 1. Съобщение, което осведомява за някое положение или за някаква дейност; сведение, осведомяване. 2. Отдел при редакция, библиотека и др., който дава справки по определени въпроси. 3. Сведения за обкръжаващия ни свят и ставащите в него процеси, които възприемат живите организми, кибернетичните машини и други в информационни системи по време на работа; в кибернетиката – количествена характеристика на съдържанието на дадено съобщение с оглед то да може да бъде предавано по някаква съобщителна система или запазено в помнещото устройство“.

Андрейчин, Л., Л. **Георгиев**, Ст. **Илиев**, Н. **Костов**, Ив. **Леков**, Ст. **Стойков**, Цв. **Тодоров**. Български тълковен речник. 4. доп. и прераб. изд. София: Наука и изкуство, 2004. 1094 с. На с. 331 е дадено значението на „информация“: **Информация:** 1. Предадено или получено съобщение, сведение, знание за някого или нещо. 2. Служба, която дава сведения. 3. Сведения, знания за предметите и процесите в света, възприемани, натрупвани и предавани от човека, от специални устройства и др.“.

С голямо внимание и интерес бихме могли да се обърнем и към авторитетни руски източници, които по идентичен начин третират феномена, наречен „информация“:

Словарь современного русского литературного языка. Том пятый. И – К. Москва, Ленинград: Изд. Академии Наук СССР, 1956. 1920 с. На с. 418 е дадено значението на „информация“: **Информация:** Сообщение, осведомление о чем-либо“.

Ожегов, С. И. Словарь русского языка. Около 57 000 слов. 10 стереотипное изд. Москва: Советская энциклопедия, 1973. 846 с. На с. 232 е дадено значението на „информация“: **Информация:** 1. Сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами (спец.). 2. Сообщения, осведомляющие о положении дел, о состоянии чего-н“.

Терминологический словарь по информатике. Ответственные за випуск И. В. Тихонова, Н. Ф. Игнатова. Москва: Международный центр научной и технической информации, 1975. 752 с. На с. 168 е дадено значението на „информация“: **Информация:** Содержание какого-либо сообщения; сведения о чем-либо, рассматриваемые в аспекте их передачи в пространстве и времени. В более общем смысле информация – это содержание связи между материальными обьектами, проявляющееся в изменении состояний этих обьектов“.

Както стана видно от горните цитирания, етимологията на думата „информация“ е от латински произход: *„informo“* – „давам форма на“. Другата дума, която се използва – „данни“, също има латински произход: *„datum“* – „давам“, и ако ги съпоставим, ще видим, че с данни се означава физически обект, който може да бъде даден, а с информация – нещо, на което е дадена форма, интерпретирано, структурирано и т.н.

Можем да разграничим три категории (три аспекта), които се асоциират с термина „информация“:

Информацията като знание: резултатът от комуникацията.

Информацията като процес: действието; осъществяването на комуникацията.

Информацията като обект: физическият обект, предаден (получен) при комуникацията.

По-горе посочихме няколко определения за информация. Тук няма да повтаряме тези определения. На основата на формалния анализ на понятието с наименование ИНФОРМАЦИЯ може да се зададе въпросът какви са отчетливите разлики между това понятие и понятията „данни“, „знания“ и пр. За нуждите на нашите изследвания, преди да се ограничим само с определянето и анализа на някои от основните информационни атрибути, ще дадем още една универсална дефиниция за информация. И така:

ПОД *ИНФОРМАЦИЯ* ЩЕ РАЗБИРАМЕ СИГНАЛИТЕ, КОИТО ПОСТЪПВАТ ОТВЪН В ДАДЕНА СИСТЕМА, ОБРАБОТВАТ СЕ И СЕ ИЗПОЛЗВАТ ОТ НЕЯ.

ИКОНОМИКА НА ИНФОРМАЦИЯТА

Информацията като стока

За разлика от всички други стоки вие може да продадете определена информация и пак ще продължавате да притежавате толкова, колкото сте имали преди продажбата на част от нея; даже повече, защото самото осъществяване на продажба на информация поражда ново знание, ново разбиране на информацията и у продавача.

Стойност на информацията

Стойността на информационните продукти се определя от степента на използването на информацията, която тези продукти предлагат. Ясно е, че това е свързано пряко и косвено с начините за използване на информацията. Във връзка с това от гледна точка на остойностяването може да се определят два различни типа информация:

Първо: Информация, необходима за ежедневното функциониране на една организационна единица. Без наличието на такава информация тази единица не би съществувала. Тук информацията има голяма стойност и доколко процесите на нейната автоматизирана обработка ще се приемат или не, зависи от това дали тези процеси ще подобрят значително работата. Този вид информация стои в основата на т.нар. системи за обработка на трансакции (TPS – Transaction Processing Systems).

Второ: Информация, която се използва за вземането на решение. Предположението тук е, че когато има повече и „по-добра“ технологична информация, персоналът, отговорен за технологичното развитие на дадена организация потребител, ще вземе поефективно и рационално управленско решение за подобряване на технологичната инфраструктура на предприятието. Информацията от този вид е част от т.нар. Управляващи информационни системи, или Системи за подкрепа на решения (MIS – Management Information Systems и DSS – Decision Support Systems).

Докато при първия вид информация като че ли е по-лесно да се определи нейната стойност, то при втория това е доста трудно, тъй като в мнозинството случаи няма директна връзка между взетото от мениджъра (инфоброкера) решение и икономическите резулта-

ти в периода на вземане на самото решение.

Може да се направи обобщението, че стойността на информацията се определя като изход от организационни процеси. На тази основа може да се предложат няколко теоретични модела за третиране на този процес, базиращи се на:

- теорията на статистическите решения;
- груповата (TEAM) теория;
- симулационното моделиране;
- субективното оценяване на информацията.

Важно е да се отбележи, че всички теории и изградените на тяхната база модели за оценяване на стойността на информацията се базират на предположението, че информацията придобива стойност само тогава, когато се използва и съществуват условия на **несигурност** при нейното използване. Когато всичко е сигурно, всичко е известно и се знае предварително, информацията е без стойност. Ясно е например, че стойността на информацията за това какви ще бъдат след една седмица индексите на съответните финансови борси, е огромна. Нищожна ще бъде стойността на информацията за това, че например вечер се стъмва.

От друга гледна точка, стойността на информацията е пряко зависима от нейните потребители. Естествено е да се предположи, че например информацията за печелившите лотарийни билети няма абсолютно никаква стойност за този, който не си е купил лотариен билет.

Субективно оценяване на стойността на информацията

От всички теории и базираните на тяхната основа методи, методологии и модели за оценяване на стойността на информацията най-сполучливи се оказаха тези, които се основават на субективни критерии (другите три модела няма да бъдат предмет на нашия анализ). Този факт по същество „се съдържа“ още в самото определение на понятието „стойност на информацията“ (**стойността на информацията зависи от степента на използването ѝ**).

В много случаи този, който се интересува от стойността на информацията, не се интересува от някаква конкретна стойност (в 90% от случаите това е реална ситуация), а за него е достатъчно само да знае дали едно, или друго определено количество инфор-

мация ще се окаже полезно, за да се свърши определена работа.

Съществуват няколко метода, на които се базират критериите и процесите за субективно оценяване на стойността на информацията:

а) опит, интуиция на оценяващия;

б) използване на аналози (системата **БИСЕР**, разработена в Централния машиностроителен институт, София, България, в края на 80-те години на XX век);

в) едно обобщение на тези субективни методи, базиращо се на мнението на експерти, е методът **ДЕЛФИ**;

г) чрез средствата на изкуствения интелект, например **Експертни системи**.

Цена на информацията

Някои автори застъпват тезата, че цената на информацията се определя главно от стойността на ресурсите, които „участват“ при нейното създаване, съхраняване, преработка и разпространение, такива като хардуер, софтуер, човешки труд и пр. От една страна, в това твърдение на пръв поглед като че ли има нещо вярно, но от друга, такова разглеждане е много ограничено и едностранчиво. Възможно е дадена информационна организация да разполага с модерна компютърна и друга високопроизводителна техника, хората, които работят в нея, да се трудят денонощно и в края на краищата по различни причини създаваната от тях информация да е БОКЛУК. Нима тази информация трябва да има висока стойност, а оттам – и цена, „защото, виждате ли, тя е създавана например чрез суперкомпютър CRAY“? Такава постановка е безсмислена, не може да се приеме сериозно и едва ли не граничи с глупост.

При определянето на цената на информацията трябва задължително да се изхожда от постановката, че тази цена е в пряка зависимост от нейната стойност. Цената е конкретен израз на стойността.

Ако се направи погрешната крачка и се стъпи на фундамента, че цената зависи само от ресурсите, оттам нататък е много лесно да се определи нейният числов израз. Това е и лесният, наукоподобен път, по който тръгват много изследователи. Типичен пример за такова изследване е частта, засягаща ценообразуването на информацията, на иначе много добрата книга Information Systems Management –

Analytical Tools & Technics. 1985, Elsevier Science Publishing Co Inc., написана от Филип Ейн-Дор и Карл Р. Джонс.

Съвременното, подкрепено от практиката виждане за определяне на цената на информацията изхожда от обстоятелството, че като реална същност, информацията е ресурс и основните методи за нейното ценообразуване трябва да бъдат пазарните. Механизмът за определяне на цената на информацията трябва да бъде такъв, какъвто е и за определяне на нейната стойност.

ИНФОРМАЦИОННА СРЕДА – БАЗОВА КОНЦЕПЦИЯ

Една от най-динамично развиващите се области на съвременния научно-технически прогрес в световен мащаб, както в теоретично, така и в практическо-приложно направление, е информатиката. Едва ли би се намерил някой, който в този момент ясно и точно да разграничи кое е конвенционалното и кое е новото, напредничавото в нейното развитие. В общия случай това, което е било ново до вчера, днес вече е остаряло.

Ясно е, че от една страна, е трудно, а от друга, и не чак толкова практично и полезно често да се сменя една или друга установена, теоретично обоснована и даваща добри практически резултати информационна концепция. Ясно е също така обаче, че за да не се изостава, за да се върви напред, в крак със световните постижения, трябва да се правят изследвания, свързани с приложението на нови концепции, базирани на авангардни методи за третиране на информацията, и постепенно и „безболезнено“ тези концепции, отначало като „опитни образци“, а след това и масово, да навлизат в информационната, а оттам – и в социалната практика. Такава концепция, намираща все по-широко приложение и с основание претендираща за относително пълно и комплексно осветляване на проблемите, засягащи процесите на рационалното, ефективно и интелигентно създаване, обработка и използване на информационните ресурси, е концепцията за **ИНФОРМАЦИОННАТА СРЕДА**.

Много често в средствата за масова информация, а и в различни специализирани издания се използва изразът „информационна среда“. Това използване обаче носи общ, неконкретен характер и служи за означаване на обобщените процеси, свързани с третира-

нето на един от феномените на нашето време – информацията, и условията, в които тя съществува. В този си смисъл понятието „информационна среда" интуитивно е ясно за всеки субект. Това е така, защото в общия случай може да се каже, че **всичко около нас представлява информация и условия за нейното съществуване**. Въпреки че горното тълкуване на това понятие не противоречи на истината, по същество то е много размито и общо и поради това почти е невъзможно концепцията за информационната среда в този си вид да бъде задълбочено изследвана и анализирана. **Такъв вид информационна среда ние ще наричаме единна, обобщена или интегрирана.** Това предполага, че наред с обобщената би трябвало да съществуват и някакви частни, относително специфични информационни среди за означаване на едни или други информационни същности. От структурна и функционална гледна точка всяка такава частна информационна среда представлява множество от три взаимносвързани компонента:

1. Информационни фондове;

2. Информационни технологии;

3. Човешки фактор, проявяващ се в интеракциите между субектите и оборудването.

С увереност може да се каже, че тази трактовка на информационна среда, в смисъл на множество от три функционално свързани компонента, дава големи възможности за задълбочени теоретчни изследвания и практически приложения. Независимо от привидно самостоятелно обособените компоненти характерът на структурирането на информационната среда е такъв, че предполага съществено влияние на всеки от нейните компоненти върху останалите. Свързващото звено тук е човешкият фактор със своите ясно изразени три типа характеристики на поведението на субектите:

- организация на взаимодействието;
- проблеми на общуването;
- психологически проблеми.

Основните параметри на такава информационна среда са:

- **предметна област;**
- **характер на информацията;**
- **информационни потоци;**
- **вид на информацията;**
- **информационни канали;**

- **информационни дейности и процеси;**
- **обем на съхраняваната, обработваната и разпространяваната информация;**
- **потребители на информация;**
- **йерархия.**

Измененията на всеки от параметрите влияе в една или друга степен върху общото състояние на средата. Изследването им с цел анализ на информационната среда е доста сложен и трудоемък процес. Оценката на моментното състояние на всеки от параметрите може да служи само като отправна точка за такъв анализ.

Параметър, определящ в значителна степен спецификата на всяка информационна среда от този вид, е **предметната област**. В зависимост от нея се диференцират съществени различия в спецификата и на трите компонента на средата.

Можем да направим заключението, че по принцип съществува една всеобхватна интегрирана и обобщена информационна среда, в рамките на която може да се диференцират т.нар. частни, отговарящи на различните специфични предметни области информационни среди. Нашият интерес е насочен предимно към изучаване и изследване именно на информационните среди от последния тип.

С цел улесняване на разглежданията и премахване на двусмисленността, от сега нататък, когато говорим за информационна среда, ще разбираме частна такава, съществуваща и развиваща се в условията на определена конкретна предметна област.

И така:

Информационната среда представлява съвкупност от информационни фондове, информационни технологии и интеракциите между хората и оборудването, осигуряващи социалната инфраструктура за обществено полезна реализация на един или друг специфичен информационен процес в рамките на определена предметна област.

От дадената по-горе дефиниция става ясно, че в зависимост от характера на информационните процеси, за които тя се отнася, информационната среда в общия случай би трябвало да носи съответната специфика.

Нека съвсем накратко да оформим общата картина на една информационна среда:

- **Информационни фондове** – първият компонент на среда-

та тук се представя от специализирани бази данни (или други информационни структури), съдържащи различна информация, от една страна, даваща достатъчно пълна, а от друга, само сигнална информация за определени решения. Важна характеристика на информационните фондове е тази, че наред с информацията, записана на магнитни носители, в преобладаващото мнозинство от случаите се съхранява и отделен фонд (на хартиени носители, на микрофишове или на видеоленти и дискове), съдържащ пълните досиета на представените данни. Съвременна тенденция тук е да се изграждат т.нар. свободно текстови и пълнотекстови бази данни. Напоследък, във връзка с повсеместното използване на мрежи от персонални компютри (ПК), се забелязва тенденция за преминаване от големи, глобални, към малки, локални и към т.нар. разпределени бази данни, съдържащи информация само за определени класове информационни ресурси.

• **Информационни технологии** – може да се каже, че този компонент на средата е относително инвариантен по отношение на различните предметни области. Въпреки това обаче при него също се наблюдава определена специфичност, дължаща се на конкретните условия за реализация на информационната среда. Спецификата на информационните технологии се определя, от една страна, от характера на информационните процеси, необходими за обработка на уникалните информационни фондове, и от друга, предимно от методите и начините за събиране и разпространяване на информация. Дискутирайки проблемите на информационните технологии, нека още веднъж да подчертаем специфичното значение на технологиите за подбор, събиране, анализ и оценка на информация. Много е важно да се разбере, че от правилния подбор на информацията в голяма степен зависи качеството на цялата информационна среда. **Възможно е в резултат на ефективния подбор на информацията да се стигне до момент, когато специалистите, отговорни за работата на средата, анализирайки информационните фондове, са в състояние да подскажат на производителите нови технологични решения**.

• **Човешки фактор** – последният по място, но не и по значение компонент на информационната среда е човешкия фактор, изразяващ се главно в интеракциите както между отделните категории специалисти, така и между тях и оборудването на средата. Тези

интерактивни процеси пронизват от край до край информационната среда и имат както технически, така и социален характер. Технически те са пряко свързани със съответните информационни технологии и фондове. От социална гледна точка интерактивният диалог представлява своеобразен феномен, отразяващ както нивото на развитие на съответната научна, технологична и техническа база, така и нивото на развитие на интелектуалните способности, мирогледа и социалната ангажираност на отделния индивид, на колектива и на обществото.

Този факт от своя страна определя една от главните особености на интерактивното взаимодействие между човека и оборудването. Тази особеност се характеризира с изискването за водене на диалог, отчитащ високото професионално равнище на специалистите, участващи в него, както на „входа“ на средата, така и на нейния „изход“.

Важно е също така да се отбележи, че специалистите по поддръжката на информационната среда трябва да притежават много добра професионална подготовка и квалификация, за да не бъдат само статисти при натрупването, обработката и разпространението на информацията, но активно да участват при формирането на крайния информационен продукт на средата.

Говорейки за социалната ангажираност на даден индивид или колектив, не можем да отминем въпросите, засягащи един по-широк кръг от проблеми относно осигуряването на подходящи условия за съществуването и развитието на информационната среда. Тук имаме предвид въпросите, отнасящи се до създаването на подходящи организационни звена, в рамките на които да се развиват определени специфични информационни среди.

Опитът показва, че най-подходящи за тази цел се оказват различните видове специализирани информационни центрове. Съществуват няколко характерни особености, които отличават информационните центрове от другите видове организационни структури. Тези особености са следните:

1. Информационните центрове са ориентирани винаги към точно определени информационни дейности;

2. Целите на информационните центрове са тясно обвързани с целите и задачите на организационните структури от по-високо ниво, в рамките на които те съществуват;

3. Обикновено преобладаващата част от персонала на информационният център не са информационни специалисти, а притежават специалности и квалификации, отговарящи на специфичната предметна област;

4. Информационните центрове имат гъвкава финансово-пазарна политика;

5. Информационните центрове почти винаги обслужват относително хомогенни и добре дефинирани групи от потребители.

Проблемите за съществуването и развитието на информационна среда в рамките на различни организационни структури и в частност в рамките на едни или други специализирани информационни центрове са предмет на много и различни изследвания. Основна предпоставка за тези изследвания е практическата значимост на въпросите, засягащи рационалното и интелигентно управление на различните по вид, структура и функционално предназначение и нарастващи с огромни темпове информационни ресурси. Едно от първите изследвания в тази област е на Caras. Използвайки системата GPSS и на базата на симулационния език GPSS III той извършва операционен анализ на относително малък информационен център. По-късно Schroer създава симулационен модел за изследване на действащия информационен център на NASA. Целта на неговото изследване е да се оцени текущата ефективност на работата на този център и да се дадат идеи и насоки за качествено подобряване на дейността му. Един от полезните резултати беше разкриването на големите потенциални възможности на информационния център на NASA за т.нар. вторичен трансфер на знания. Заслужават внимание също работите на Rourke и Howes, Curk и Minker, Ware и Schuenemeyer, Lientz и др. Най-голям интерес за нас представляват ранните, основополагащи трудове на J. Jolly, който е един от пионерите на изследванията, свързани с организационните структури за съществуване и развитие на информационен трансфер на технологии. Цитираните дотук изследвания и опитът от практическото извършване на дейности по информационен трансфер категорично показват, че ефективност се наблюдава само тогава, когато информационният трансфер се осъществява от относително неголеми, предметно ориентирани информационни центрове.

Интегрирането на информационния трансфер в рамките на информационни организации с широк профил на обслужване води

до ниско качество на работата и създава реални предпоставки за спъване на технологичното развитие. Друг, не по-маловажен проблем е проблемът за икономическата заинтересованост. Световният опит в това направление показва отдавна известните, но често пренебрегвани истини, че ефективност може да има само тогава, когато цялата дейност по информационното обслужване е поставена на икономическа основа. Последното не пречи, а напротив, създава по-благоприятни условия за изпълнение на стоящите пред специализираните информационни организации социални поръчки и задачи.

МОДЕЛИ ЗА ОПИСАНИЕ НА СТРУКТУРНО-ФУНКЦИОНАЛНИТЕ КОМПОНЕНТИ НА ИНФОРМАЦИОННА СРЕДА

Основните идеи, методи и средства в теорията и практиката на информационната среда на концептуално ниво може да се обобщят в станалите вече класически три йерархични модела.

Първият от тези модели се формира в рамките на теорията на информацията, като резултат от пионерните изследвания на К. Шенън, и отразява тенденцията към оптимизация на обработката, съхраняването и разпространението на технологичната информация с цел повишаване на икономическата и социалната ефективност от развиващите се с бързи темпове технологични иновационни процеси.

Вторият обобщен модел се базира на теоретичните изследвания на Сосюр, Фреге, Мински и др. в областта на семиотиката и съответстващите ѝ съвременни практически резултати. Този модел отразява тенденцията към по-дълбоко проникване не само в синтаксиса, но и в семантиката на информационните процеси и на тази основа създава предпоставки за по-пълно, точно и адекватно отразяване на смисловото значение на технологичната информация.

В началото на 80-те години на XX век започна развитието на **трети** вид модели на информационна среда, основните идеи и методи на които се породиха в рамките на комплексното научно направление „изкуствен интелект“. Главните елементи на този модел са знанията и средствата за тяхното представане и обработка. Целта на модела се асоциира с:

Първо: Интензивна научноизследователска работа в областта на интелектуализацията на информационните технологии;

Второ: Създаване на реални възможности за имитиране на творческата човешка дейност и реализиране на приложни системи за автоматизирано решаване на определени класове и типове интелектуални задачи.

Този модел синтезира основните характеристики на първите два модела, развивайки тези характеристики и добавяйки към тях по естествен начин интегрирания теоретико-методологически апарат на философията, психологията, лингвистиката, кибернетиката и информатиката, формализирайки механизмите на естествения човешки интелект.

АНАЛИЗ И УПРАВЛЕНИЕ НА НЕСИГУРНА ИНФОРМАЦИОННА СРЕДА

Информационна среда – несигурност

По-горе дефинирахме основните понятия, засягащи информационната среда като общо понятие, обръщайки задълбочено внимание на факта, че независимо от спецификата на различните предметни области от реалната действителност информационната среда остава инвариантна същност както по отношение на съставящите я компоненти, така и по отношение на връзките между тях. От друго естество обаче са въпросите, отнасящи се до свойствата на отделните компоненти, свързани с конкретното „проявление“ на информационната среда. Във връзка с това показахме и дискутирахме характерните, присъщи само на информационната среда специфики. Не е трудно да се обоснове, а още по-малко трудно е да се забележи, че информационната среда като обща категория съдържа голям процент несигурност в различните си аспекти на проявление. Несигурност, и то от различно естество, има както в средата като цяло, така и в отделните ѝ компоненти. Ние няма да се връщаме отново към дискутиране и анализ на основните причини за появата на несигурността, но ще обърнем внимание на проблемите, отнасящи се до несигурността при анализирането на информационната среда, като разделим тези проблеми на три нива:

Първо: Несигурност в основните идентифициращи характеристики на средата;

Второ: Несигурност в компонентите ѝ;
Трето: Несигурност в информационната среда като цяло.

Нивата на анализа на несигурността кореспондират с йерархичната структура на информационната среда.

I. Основни идентифициращи характеристики

Компонентите на информационната среда притежават следните основни идентифициращи характеристики:

- субекти;
- оборудване;
- процедури;
- обекти (цели);
- комуникации;
- динамика;
- информация (данни, знания);
- вход;
- изход;
- ограничения;
- контрол.

Нека да разгледаме тези характеристики и да анализираме проявленията на несигурността при всяка от тях, обръщайки внимание на спецификата, отнасяща се конкретно до информационната среда.

1. Субекти. Хората са най-важната, основна идентифицираща характеристика на всяка информационна среда. Тук те се делят на три главни групи:

- потребители;
- изследователски и обслужващ персонал;
- управляващ персонал.

Независимо от това функционално деление представителите на всички групи „притежават“ определен процент несигурност, дължаща се, от една страна, на естеството на човешката психика и съзнание, а от друга, на интеракцията им с останалите основни идентифициращи характеристики на средата.

Характерно за представителите на първата група е, че в случая на информационната среда преки потребители на информационните ресурси на средата са само тясно определени категории от хора – специалисти в различните технологични области. Тази харак-

терна особеност на потребителите е база за диференциране на информационните технологични ресурси с всички произтичащи от това елементи на несигурност.

По принцип субектите от втората и третата група трябва да представляват един обединен монолитен колектив от специалисти с различни специалности и интереси, поставили си една и съща цел. При информационната среда се забелязва ясно разграничаване на функциите на специалистите от изследователския и обслужващия екип. Тези от тях, които се занимават с изследователска дейност и дейност по развитие на средата, трябва във всеки момент да притежават знания, отговарящи на най-новите постижения на науката, техниката и технологиите в съответните тясно специализирани технологични области. Последното обаче по обективни причини невинаги е постижимо, а тази непостижимост от своя страна води до определени съмнения, асоциирани с несигурност по отношение на „вложените" в средата субективни знания и информация.

За субектите от обслужващия персонал е характерно, че те не трябва да бъдат странични наблюдатели на процесите, протичащи в информационната среда, и да упражняват върху нея само рутинни действия, а пряко и активно да участват във формирането на потребителските изходи. Поради естеството на метода, на който ние базираме нашите изследвания, понятието „обслужващ персонал" тук има формално значение и то служи само да покаже кои от субектите имат непосредствен допир до информационните ресурси, без да утвърждава, че тези субекти имат само рутинни функции.

От управляващия персонал се изисква да притежава знания, умения и навици, позволяващи му да упражнява ефективна координация както между компонентите на средата, така и между средата и външните условия, в които тя съществува и се развива. Важна особеност, отнасяща се конкретно до информационната среда, е, че за всяка отделна технологична област трябва да има специалист, който пряко да отговаря за нея и да управлява нейното развитие в рамките на средата. Всички такива специалисти са задължени да познават в детайли и да оказват въздействие само на специфичните подцели, които са в рамките на тяхната оторизация. Наложително е съществуването на главен мениджър, които да знае и да има пълномощията да управлява основната цел на средата.

2. Оборудване. Обикновено, като се каже „оборудване", много

от нас свързват това понятие единствено с компютрите и тяхната периферия. В рамките на една информационна среда обаче към оборудването трябва да бъдат причислени всички технически средства, като апаратура за микрографика, пишещи машини, текстови процесори, комуникационни устройства, специализирана графична техника, аудио- и видеоапаратура, CD-ROM устройства, DVD и въобще всичко, на което се базират информационните технологии. От теорията, а и от практиката е известно, че всяко устройство се характеризира с определена степен за надеждност. Тези степени за надеждност се свързват по естествен начин с понятието „несигурност“ в различните му форми и аспекти на проявление.

3. Процедури. Процедурите са всички „овеществени“ методи, на основата на които функционира дадена информационна среда. Казано компетентно, това са практически реализираните методи за събиране и анализ на информацията, за обработка на входната информация и съдържанието на вече изградените информационни фондове, за да се получат исканите на изхода резултати. Като цяло процедури са проектирането на един жизнен цикъл на информационна среда, на изхода (отпечатване на запис на магнитен носител, телекомуникация и пр.), всички човеко-машинни интеракции и др.

На основата на процедурите се изграждат и различните информационни технологии. Дотолкова, доколкото в една информационна среда се използват някои специфични методи, главно за подбор, анализ, оценка и разпространение на информацията, реализираните на тяхната основа процедури също носят белезите на специфичността. Що се отнася до несигурността, то при този вид основни, идентифициращи за информационната среда характеристики тя е от общ характер.

4. Обекти (цели). Всяка информационна среда, в зависимост от предметната област, в която съществува и която обслужва, има характерна, специфична само за нея цел. Тази цел по правило е декомпозирана както хоризонтално, така и вертикално на отделни подцели, които ще наричаме обекти. В рамките на информационната среда обектите се „припокриват“ с различните технологични направления. Поради причини от различно естество при такива, като например приоритетното развитие на дадени технологични направления за точно определени периоди от време, се установяват качествени и количествени различия както в сферата на обек-

тите, така и в определянето и използването на необходимите ресурси за тяхното постигане (или изграждане). Този факт представлява предпоставка за поява на несигурност, засягаща дефинирането и развитието на главната цел на информационната среда.

5. Комуникации. Една от съществените особености на информационната среда е нуждата от комуникации. Комуникации както вътрешни, между отделните компоненти, така и външни, между информационната и околната среда. Без вътрешните комуникации средата не би могла да съществува, а без външните тя не би получавала, а така също и не би давала информация, т.е. информационната среда би се превърнала в ненужен, самоцелен продукт.

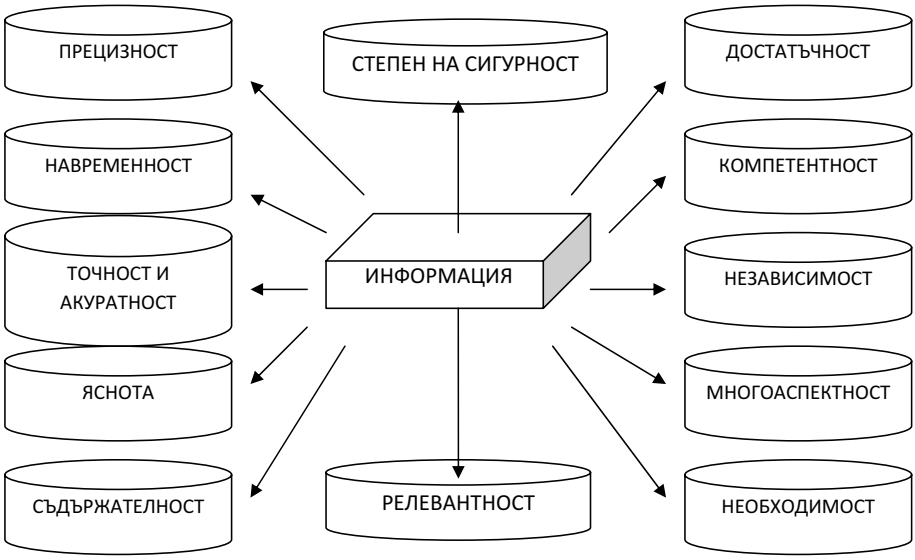
Както вътрешните, така и външните комуникации в една среда носят специфичните белези на несигурността. Несигурност, която, от една страна, се определя от сложността на връзките между отделните технологични направления и наличните информация и знания, чрез които те се представят, а от друга, от многофакторността при реализацията на изходите на информационната среда, кореспондиращи пряко с технологичната и социално-икономическата иновационна политика на обществото.

6. Динамика. Всяка информационна среда трябва да има възможност да се променя динамично в зависимост от измененията на условията, в които съществува, или от измененията на някои от нейните собствени компоненти.

Под „динамика“ ще разбираме способността на информационната среда да се променя, поддържайки едно и също ниво (или подобрявайки нивото) на работоспособност и ефективност. Динамиката, като основна идентифицираща характеристика, играе съществена роля в информационната среда. Определено може да се каже, че такъв тип среда търпи непрекъснати изменения, базирани както на развитието на съставящите я компоненти и усъвършенстването на връзките между тях, така и на условията, в които тя реализира своите изходи. Не ще и съмнение, че тези чести промени определят и по-високата степен на несигурност, характерна за информационната среда.

7. Информация (данни, знания). След субектите информацията е втората по значение основна идентифицираща характеристика на информационната среда. Образно казано, това е „главният флуид“, който се движи в посока **към, вътре** и **от** информационната среда.

Сами по себе си всички проблеми и аспекти, засягащи понятието „информация“, са основа за написването на не един самостоятелен труд (такива има стотици). За нуждите на нашите изследвания тук ще се ограничим само с определянето и анализа на някои от основните информационни атрибути. Тези атрибути са представени на фиг. 1.



Фиг. 1. *Основни атрибути на информацията*

Когато идентифицираме конкретни атрибути на информацията, ние винаги задоволяваме изисквания съобразно субективните си нужди. В този случай казваме, че информацията ни удовлетворява – когато в процеса на търсенето установим, че сме намерили дадена информация, от дадено място, за определен тип потребители, в рамките на определено време. На някои от атрибутите на информацията е трудно да се установи състоянието и на тази основа е почти невъзможно да бъдат измерени. Всичко тук зависи от това, което е полезно за потребителя на информацията.

Ето и значенията на атрибутите на информацията, на които спираме вниманието си:

• Прецизност – този атрибут показва степента на детайлизация на информацията, отговаряща на изискванията на потребителите;

• Навременност – характеризира получаването на информацията в рамките на точно определен интервал от време;

• Точност и акуратност – определя степента на отсъствие на грешки от формално и логическо естество;

• Яснота – характеризира наличието или липсата на излишна, ненужна информация;

• Комплексност – характеризира количеството и качеството на информацията, отнасяща се до конкретен проблем;

• Независимост – този атрибут определя степента, до която информацията се предоставя на потребителите без изменения, продиктувани от външни и странични фактори;

• Многоаспектност – показва степента, до която определена информация покрива различни, но свързани един с друг аспекти на потребителската заявка;

• Необходимост – определя мотивационната същност на информационното търсене;

• Съдържателност – този атрибут показва отношението на информативността на информацията към нейния обем. Тоест по-съдържателна е тази информация за определено събитие, явление или процес, която е представена в по-малък обем;

• Достъпност – определя възможностите за използване на иначе налична информация;

• Релевантност – този атрибут има комплексен характер. Той показва доколко информацията отговаря на тази, заявена от потребителя;

• Степен на сигурност – както релевантността, така и този атрибут има комплексен характер и в случая той кореспондира пряко с условията, даващи основание да кажем, че дадена информация има определена степен на сигурност или респективно несигурност (ниво на класификация).

8. Вход. При анализирането на една информационна среда трябва да се има предвид, че „входът“ на тази среда, определен като идентифициращa характеристика, е понятие с много по-общо значение, отколкото например директното или индиректното въвеждане на информация в компютъра. Тук това понятие трябва да се асоциира (свърже) с такива дейности като активно търсене на информация и знания, идентифициране на информационните източници, обработка, анализ и оценка на постъпващата информация и изграждане на информационните фондове на Средата. **За всяка информационната среда е характерно това, че нейният**

„вход“ по същество представлява сложна оценъчна система, съдържаща както характерните особености на информацията, представена от специфичните информационни източници, така и механизми за експертно анализиране и оценка. Сигурността на Входната информация на Средата в голяма степен определя и сигурността на информацията на нейния изход.

9. Изход. Всички резултати, получени от работата на информационната среда, се наричат неин изход. Към изхода обаче трябва да се прибавят и тези допълнителни неща, като книги, брошури, микрофишове, видеофилми и др., които са в пряка връзка и зависимост от директните резултати. Изходът при информационната среда се определя от специфичното потребителско търсене, имащо пряко отношение към определена технологична иновационна политика. Сам за себе си изходът притежава перманентна несигурност, като тази несигурност може да бъде увеличена или редуцирана в процеса на адаптирането на изходните резултати за задоволяване на конкретните нужди на потребителите.

10. Ограничения. Всяка информационна среда трябва да има строго дефинирана област на съществуване и развитие. Тази област се определя от не дотам строгите граници на иновационните технологични процеси. В общия случай може да се каже, че тези граници представляват и главните ограничения за Средата. Те фактически се явяват ограничения на отделните компоненти и параметрите, които ги описват. Тъй като по принцип границите на дефиниционната област на Средата не може да се определят точно, този факт сам по себе си е предпоставка за съществуването на несигурност.

11. Контрол. Под „контрол“ като основна идентифицираща характеристика на информационната среда ще разбираме лимитираните или инцидентни проверки на интерактивните процеси между хората и оборудването в процеса на изпълнение на различните процедури. Контролът при информационната среда се характеризира с висока степен на сложност, дължаща се главно както на оперирането с разнородна информация от високо качество, така и на много високата професионална подготовка на потребителите ѝ. Безспорно сложността на този процес води със себе си и по-висока несигурност.

II. Компоненти

Ще се наложи още веднъж да припомним, че три са главните компоненти на информационната среда:

- **информационни фондове;**
- **информационни технологии;**
- **взаимодействие човек – оборудване (компютър)**.

По-горе ние анализирахме основните идентифициращи характеристики на информационната среда и установихме, че би трябвало да очакваме подобна несигурност да се среща и при компонентите на Средата, защото те се базират преди всичко върху тези характеристики.

И наистина, определено може да се каже, че всеки от компонентите потенциално е носител на несигурност, но тази несигурност в общия случай не е само в резултат на сбора от несигурностите на отделните идентифициращи характеристики, а нейното формиране в значителна степен се влияе и от характера на организацията на връзките и комуникациите между идентифициращите характеристики в рамките на отделните компоненти.

1. Информационни фондове. Несигурността при този компонент на информационната среда се описва преди всичко в термините на различните мерки. В зависимост и на основата на изменението на характера и структурата на технологичната информация и знанията, съдържащи се в тези фондове, отчетливо се забелязва постепенно изместване на ударението, определящо спецификата на несигурността и нейното измерване, от вероятностните мерки (частен случай на размитите мерки) в посока към мерките за дисонанс, конфузия, неспецифицираност и U-несигурност.

2. Информационни технологии. Информационните технологии по принцип са компонент на информационната среда, които остават относително инвариантни по отношение на предметната област и външните условия за съществуване и развитие на Средата. Дотолкова, доколкото този компонент се базира главно на процедурите и оборудването, несигурността при него се явява предимно във форма, удобна за третиране (измерване) с класическите мерки за несигурност.

3. Взаимодействие човек – оборудване (компютър). От гледна точка на несигурността, от една страна, това е компонентът, притежаващ най-голяма несигурност, а от друга страна, методите и прак-

тическите процедури за редуцирането ѝ са най-лесно осъществими. В крайна сметка основната тежест както за определянето на степента на несигурност, така и за нейното „разрешаване“ пада върху единия от интерактивно взаимодействащите си елементи – човека. От неговата компетентност, интелект и умения по същество зависи доколко може да се каже, че информационната среда като цяло притежава една или друга степен на несигурност. Характерът на несигурността при този компонент е предимно такъв, че най-подходящи мерки за нейното измерване се оказват мерките за размитост.

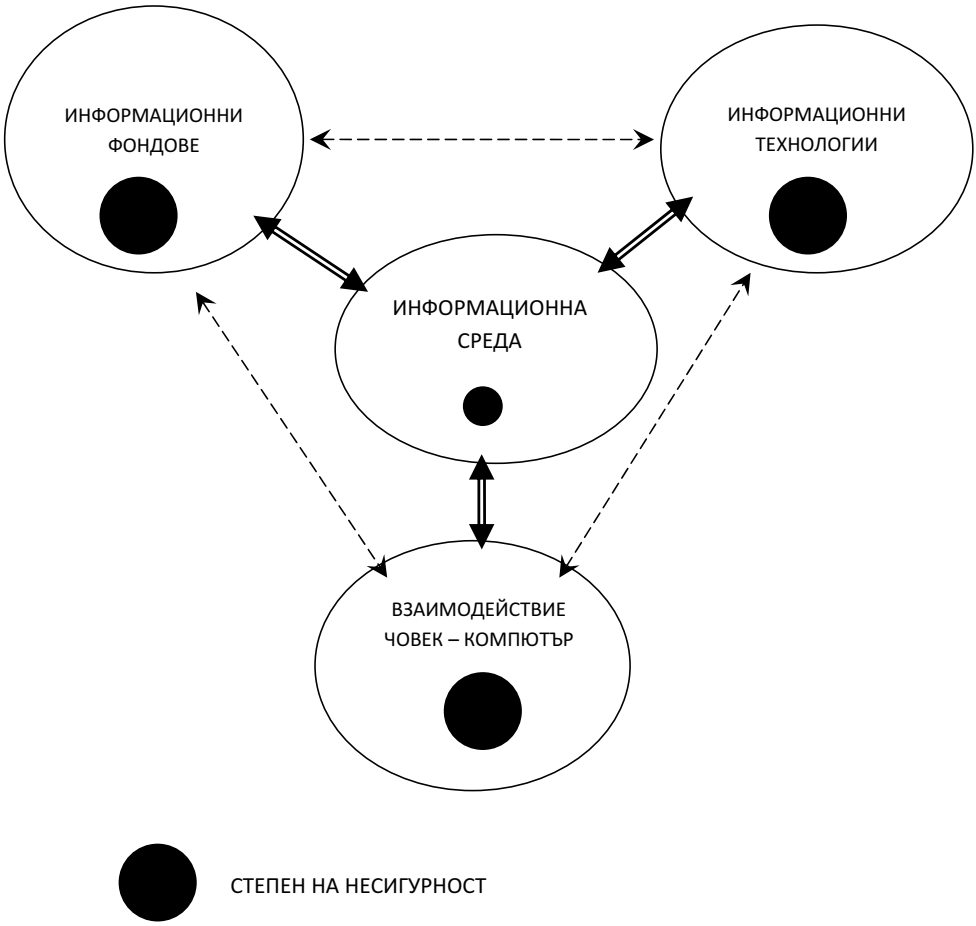
III. Информационна среда

Изхождайки от постановката, че една добре развита система е много повече от обикновения сбор от съставящите я компоненти, можем да твърдим, че съществува несигурност, но тази несигурност в една или друга степен е управляема. **Под „управляемост на несигурността“ ще разбираме сбора (сумата) от всички действия, водещи до нейното редуциране.** Управляемостта на несигурността, а оттам – и на информационната среда като цяло, се дължи главно на постоянно усъвършенстващите се организационно-функционални структури на информационните среди от този тип и предимно на факта, че в рамките на тези структури работят специалисти и мениджъри с висока професионална квалификация.

Определянето на характера на несигурността в една информационна среда има голямо значение както за качественото анализиране и динамичните оценки на тази среда, така и за решаването на проблемите, засягащи нейното ефективно и интелигентно управление.

В зависимост от смисъла, влаган от различните автори при определянето на отделните ѝ компоненти, информационната среда като понятие има дискусионен характер. Може би това е една от причините, поради които изследователите не се заемат с проучването на проблемите, засягащи системния анализ и развитието ѝ. Погледнато от друга гледна точка обаче, надали съществуват научно знание и приложна област, които да не съдържат известен процент несигурност, противоречия, несъответствия, колизии, съмнения и пр. Ако следваме първото виждане, т.е. виждането, че нищо не е сигурно и за да се продължи напред, трябва да се решат всички спорни въпроси, това би означавало, „измивайки си ръцете“, да застанем на позициите на странични наблюдатели, пасивно

изчаквайки решаването на принципно неразрешими проблеми. Нашата позиция обаче е друга, съответстваща на втората гледна точка, и от тази позиция ще направим опит да анализираме различните етапи, фази, моменти и процеси от развитието на информационната среда. Предварително трябва да обърнем внимание, че изводите, които ще направим в процеса на анализа, в голямата си част имат значение за каквато и да е информационна среда.



Фиг. 2. *Несигурност в информационна среда*

Няма нищо свръхестествено, уникално, нито пък необикновено при процесите на анализ на една информационна среда в нейното развитие. От принципна гледна точка това е базова методология, приложима за всяка сложна динамична система. Важното при

тази методология обаче е строго да се спазват определени правила, принципи и последователности.

В зависимост от избора на различни критерии съществуват няколко общи подхода за анализ:

- сруктурен;
- неструктурен;
- системен;
- несистемен и др.,

които тук е излишно да дискутираме по-подробно.

На основата на избраното централизирано или нецентрализирано (разпределено) развитие на информационната среда и предварително определените критерии се предпочитат едни или други подходи за анализ. Във връзка с това трябва ясно да се разбере, че процесите на анализ и развитие на информационната среда са неразривно свързани и всякакъв опит за индивидуализиране на изследванията, клонящи в едната посока, биха дали резултати, далеч от реалните.

Нуждата от системен подход за анализ на развитието на една информационна среда се определя от следните фактори:

1. Постоянно развитие и усъвършенстване на целите, определящи се от бързо променящите се условия на иновационните технологични процеси;

2. Потенциална възможност за подобряване на обслужването на потребителите на основата на смяната на управленските условия, оборудването, технологичните решения и др.;

3. Научни открития, технологични и технически изобретения и нововъведения. Новите открития и изобретения са катализатори, а в някои случаи и инициатори за създаването и развитието на нови (или преминаването към следващ жизнен цикъл) информационни технологични среди;

4. Икономически условия – в общия случай те се определят от възходящото постъпателно развитие както на специализираната организация, в чиито рамки съществува информационната среда, така и на цялостната икономическа система;

5. Организационно планиране – анализите и развитието на информационната среда много често представляват част от краткосрочни или дългосрочни планове;

6. Конкуренция – този фактор не е за пренебрегване, защото

той директно, а в много случаи и индиректно играе съществена роля при формирането на нуждата от анализ и развитие на информационната среда;

7. Пазарно търсене – повишаването на социалния статус на дейностите, свързани с трансфера на технологии, и в частност увеличаването на броя на заявките за трансфер на технологични знания са важен фактор, даващ тласък на процесите на анализ и развитие на информационната среда;

8. Задълбочаване и развитие на международните търговски отношения;

9. Правни съображения – този фактор има пряка връзка с измененията на законодателствата, свързани с правните промени, продиктувани както от научно-техническия прогрес, така и от текущия политически статус.

Много често явление, което се наблюдава при големи, сложни и комплексни системи, е наличието на дисхармония между системите и условията, в които те съществуват и за съжаление, се развиват. Тази дисхармония е в резултат на неправилен, или по-точно казано, некомпетентен анализ както на развитието на системите, така и на съпътстващите ги условия. Развиват се например големи индустриални мощности, а не се вземат под внимание фактите, че отсъстват необходимите енергийни източници или че тези мощности в продължение на голям период от време ще оказват отрицателно въздействие върху демографското и екологичното равновесие. Същото се отнася и за процесите на анализ и развитие на информационната среда като една комплексна система, съдържаща голям заряд социално въздействие. Тези процеси задължително трябва да са съобразени със съпътстващите информационната среда външни условия. Когато се анализира развитието на Средата, изводите и препоръките трябва в известна степен да изпреварват условията. Това е необходимо изискване, защото за определен период от време съпътстващите условия остават относително постоянни.

Една друга, може би на пръв поглед странична, но също важна предпоставка за задълбочено анализиране на развитието на информационната среда е тази, целяща действително полезното развитие на Средата, в посока на усъвършенстване на нейната ефективност (в частност на интелигентността ѝ) за сметка на често срещащото се напоследък увлечение по атрактивността.

Жизнена цикличност на информационната среда

Съществуването на реалния свят, обвързан с разума на хората, предполага съществуването и развитието на самостоятелни или припокриващи се информационни среди за различните сфери на живота, предмет на съзнателната човешка дейност. Обръщайки поглед към миналото, оценявайки настоящето и предвиждайки бъдещето, можем с увереност да твърдим, че във всеки период от човешката история е съществувала, съществува и ще съществува в различни форми, видове и структури реалната комуникационна същност, наречена **информационна среда**.

Независимо от характера, формите на представяне и организацията на информацията и знанията, независимо също така от примитивните или пък суперсложните процедури за обработка на тези информация и знания ние имаме пълно основание да наречем тези две отделни категории (форми и организация на представяне и процедури) съответно информационни фондове и информационни технологии. Що се отнася до интеракцията човек – компютър, то взаимодействие, в известна степен подобно на това, е съществувало винаги в съзнателното, а в някои случаи и в несъзнателното използване от хората на наличните информационни ресурси. В това отношение не бива да сме догматици, мислейки, че компютърът (колкото и да е усъвършенстван) е върхът на творческия човешки гений. Сигурно в немного далечното бъдеще в процеса на обработката и използването на информация и знания нашите наследници ще взаимодействат активно със създадена от тях техника, принципно различна от компютърната.

Информационната среда е силно обвързана със съзнателната човешка дейност. Не е случайно хрумване и определянето на наименованието на тази част като „Жизнена цикличност...“. С това наименование искаме още в самото начало да заострим вниманието върху спираловидното, възходящо развитие на една от основните комуникационни същности – информационната среда.

Ясно е, че е много трудно, а дори и невъзможно в исторически план да се анализира развитието на информационната среда в цялата ѝ същност. Задачата, която сме си поставили, е по-скромна и тя опира само до анализа на развитието на един жизнен цикъл на информационната среда. Този анализ ще направим, използвайки методите и методологиите на т.нар. класически техники за научно

решаване на проблеми (problem solving). Въпреки че съществуват много вариации на тези техники, в общия случай те може да се обединят на основата на следните стъпки:

1. Дефиниране на проблемите (поставяне, изменение на целите);
2. Анализ на проблемите;
3. Търсене и подбиране на алтернативни решения;
4. Тестване (верификация) на избраното решение;
5. Прилагане в практиката.

Анализирайки развитието на информационната среда, с цел ясно да се разграничат специфичните дейности в рамките на жизнения цикъл, ще разделим този цикъл на отделни, относително самостоятелни фази и дейности:

I. ФАЗА НА ФОРМИРАНЕ (УСЪВЪРШЕНСТВАНЕ) НА ЦЕЛИТЕ

Тази фаза се асоциира с установяването на изискванията за идентифициране на задачите, които трябва да бъдат решени, и евентуално избор или разширяване на кръга от потенциалните потребители на технологична информация и технологични знания. Тук трябва да се даде отговор на два главни въпроса:

Първо: Какви ще са очакваните резултати и каква ще е ползата за създаването на нова или от измененията на съществуваща информационна среда?

Второ: Какви ще са индивидуалните разходи за развитието на средата и за колко време те ще се покрият от очакваната полза?

Няколко вида условия могат да инициират нуждата от създаването на нова технологична информационна среда или да станат база за възходящо развитие на съществуваща такава:

- промяна на икономическите условия;
- научен или технологичен скок;
- дългосрочно планиране;
- нов сервиз;
- промяна на пазарното търсене (в това число на международните пазари);
- наличие на проблеми при съществуваща информационна среда;
- нови законови и правни регулации.

Основните компоненти и процеси във фазата на формиране (преформулиране) на целите са следните:

1. Подготовка на „заявка". Това е първата стъпка, която инициира искането за подобряване на съществуващата информационна среда или за създаването на нова такава. Няма ограничения, засягащи източника на искането. „Заявката" може да бъде направена от всеки специалист (група от специалисти), от всяко звено или организация. Типичен пример за такова „писмо заявка" е писмото, обосноваващо създаването и развитието на информационната среда за трансфер на технологии в рамките на новата организационна структура „Информационен център за трансфер на технологии – ИНФОРМА", София, България.

2. Предварителна оценка на „заявката". Подготвеното на първата стъпка обосновано и аргументирано искане се изпраща до отговорната научно-административна инстанция (обикновено в тези отговорни инстанции съществуват специални оценъчни комисии), която трябва да ранжира предложенията на основата на някои от следните критерии:

- наличие на действителна необходимост (аргументи и доказателства, че съществуващата информационна среда не е адекватна на новите условия и изисквания);
- доколко ясно и разбрано е описано как и по какъв начин ще бъдат решавани съществуващите и бъдещите проблеми в рамките на новата или подобрена информационна среда;
- аргументация на възможностите за решаване на възникналите проблеми в рамките на определено време и средства.

3. Съставяне на план за предварителни изследвания. Този план се прави след евентуална положителна оценка на „заявката" и неговото предназначение е да даде направления за работа и възможност за контрол. При съставянето му трябва да се обърне внимание на:

- желани (очаквани) резултати от работата – Какъв резултат ще се получи? Кога и как този резултат ще излезе наяве?;
- разпределение на времето за работа;
- определяне на средствата, необходими за реализацията на проекта;
- определяне на човешките ресурси и необходимите сръчности, умения и знания на хората, работещи на тази фаза.

4. Определяне на потребителите и техните нужди. При извършването на тази стъпка основно трябва да се ръководим от следните съображения:

- идентификация на типа на потребителите – това трябва да се извърши в съответствие с характера на информационната среда, в зависимост от режимите на работа и персонала, поддържащ, развиващ и управляващ средата;
- потребностите на потребителите трябва да се екстраполират така, че да не се определят само за текущия момент, а най-малко за 5 – 10 години напред;
- идентифицирането на функционалните връзки между различните типове потребители може да стане основа за определяне на допълнителни цели, тъй като комплексните потребителски изисквания в общия случай са повече от простата сума на изискванията на отделните потребители;
- установяването на релативни (относителни) граници и лимити за нуждите на всеки потребител.

5. Дефиниране на термини. В резултат на тази стъпка трябва да се получи „речник“ с термини, които са специализирани за областта на трансфера на технологична информация и технологични знания. Този „речник“ е от отворен тип, т.е. винаги може да се допълва или коригира в процеса на работа. Значението на терминологичния речник се определя на първо място от премахването на възможността за двусмислени тълкувания на едни и същи реалности.

6. Развитие (уточняване) на целите на информационната среда. По същество основните цели на информационната среда се свеждат до даване на отговор на въпросите каква ще е ролята на средата и какво ще се прави в рамките на тази среда. Тези отговори може да се дадат на основата на описанието на следните параметри:

- изход – съдържание, физически формати, честота;
- вход – източници;
- операционни възможности;
- ресурсни ограничения;
- очаквана цена;
- географско разположение и свързаните с него комуникационни изисквания;
- съхраняване, безопасност и секретност на информационните фондове.

Разбира се, тези параметри не може, а и не трябва да бъдат детайлно анализирани на тази стъпка.

7. Определяне на ресурсните параметри, отношенията и връзките между тях. Ресурсите представляват налични или очаквани блага, които са достъпни за използване и развитие на информационната среда. Те може да се отъждествяват например с хардуер, софтуер, персонал, сгради, източници на технологична информация, канцеларско оборудване и пр. Важно е през тази фаза да се определят колкото е възможно по-акуратно и точно степените на свобода на проектантските усилия в зависимост от евентуално наложените ресурсни ограничения. За да стане това, трябва да се направи опит да се определят всички ресурси и техните ограничения в съответствие с постановката за развитие на информационната среда. Не трябва да се забравя и изискването, че ресурсните параметри трябва да се разглеждат и анализират заедно, в своята взаимовръзка, а не изолирано, защото са силно зависими един от друг.

8. Създаване на „перспективна снимка“ на външните условия, в които информационната среда ще съществува и ще се развива.

9. Идентифициране на входовете и изходите на средата.

10. Идентифициране на функциите на информационната среда. Основният въпрос, на който трябва да се отговори тук, е какво трябва да се направи, щото входът да се трансформира до полезен изход. Определянето на функциите става впоследствие база за изграждането и използването на едни или други информационни технологии.

11. Предварителен избор на възможното оборудване.

12. Подготовка на съображения относно планиране на участието на хората при изграждането и използването на отделните компоненти на информационната среда:

- описва се всеки проблем, свързан с непосредствено човешко участие;
- определят се типът и качеството на изискваното обучение.

13. Определяне на подцели, пряко свързани с контрола. Трябва да се изхожда от съображението, че контролът не е случайна цел. Той не бива да е инцидентен, а трябва да се проектира. Контролните цели трябва да се отнасят до следните области:

- текущо поддържане на технологичната информационна среда и обезпечаване на сигурна и надеждна работа;

• данни и информация – секретност и безопасност;

• регулации съобразно политиката на организацията, отговорна за информационната среда.

14. Ранжиране на целите (обектите).

15. Изготвяне на план за развитие, подкрепен с финансови изисквания.

16. Подготовка на доклад. Докладът е заключителна стъпка от тази фаза. Той трябва да съдържа информация, обособена в следните части:

• абстракт – обобщен поглед върху информационната среда;

• цели, които се поставят с изграждането и развитието на средата;

• ресурси и ограничения;

• структурно и функционално описание, придружено със съответните схеми;

• отговор на основния въпрос – как информационната среда за трансфер на технологии ще отговори на потребителските изисквания;

• икономическо въздействие върху организацията, в рамките на която се изгражда и развива информационната среда; какво ще бъде въздействието на тази среда върху организацията в рамките на информационния пазар;

• разпределение на времето за проектиране, създаване и развитие;

• цена (средства);

• терминологичен речник;

• препоръки за изготвяне на системна документация на средата;

• специални съображения относно развитие на взаимодействието човек – оборудване.

II. ФАЗА НА ДЕФИНИРАНЕ НА ПРОБЛЕМИТЕ

Одобреният доклад и цялата предварителна документация, изготвена по време на първата фаза, дават основание за развитие на т.нар. **Фаза на дефиниране на проблемите**. През тази втора фаза, от една страна, ударението се поставя върху дефинирането на основните очаквани резултати, а от друга, върху необходимите усилия за тяхното постигане. Тук се създава и фактическата структура, по която ще се гради и развива информационната среда. Последователността започва с формирането на изискванията за създаване на

колектива за работа и с дефинирането на изходите, които се очакват от потребителите. След това специфицирането продължава, докато се дефинират и входовете. Тази фаза съдържа също писмено описание на входовете, изходите, информационните фондове и пр.

На фазата на дефиниране на проблемите всички въпроси, на които трябва да се отговори, започват с **„какво“**. Въпросите, съдържащи думата **„как“**, се поставят в следващите фази. Дейностите, които трябва да бъдат извършени тук, може да се представят чрез следните стъпки:

1. Формиране на изисквания за създаване на работен програмен колектив. Тази стъпка е основа за следващата фаза, при която се извършва действителното, реално формиране (усъвършенстване) на колектива.

2. Дефиниране на ограниченията на информационната среда. Лимитите за развитие на средата трябва да бъдат прецизно определени в съответствие с възможностите на организацията, отговорна за изграждането и развитието на информационната среда.

3. Развитие на план за събиране на технологични данни, информация и знания. Има много методи за активно търсене, диференциране, събиране и предварителна оценка на технологични данни, информация и знания. Изборът на всеки от тези методи се базира на наличието на няколко фактора: пари, време, специални изисквания.

4. Развитие на изисквания за изхода на средата.

5. Развитие на изисквания за входа на средата.

6. Дефиниране на функциите и условията, от които те зависят. Това е първата крачка за обособяването на отделните информационни технологии.

7. Установяване на същността на специфичната предметна област, в рамките на която ще се развива технологичната информационна среда и която същевременно ще обслужва.

8. Изготвяне на доклад. Този доклад задължително се представя за одобрение, като се очакват следните решения:

- одобрява се работата да продължи;
- предявяват се изисквания за модификации и/или съществени промени;
- отлага се;
- прекратява се.

В доклада трябва да се съдържа прецизна, фактическа, ясна и качествена информация за следното:

- системните цели, свързани с изграждането и развитието на информационната среда – изцяло уточнени и установени;
- глобално (цялостно) описание на средата (поотделно за трите ѝ главни компонента), съдържащо представяне на спецификации;
- описание на функциите на входа, обработката и изхода;
- изискващи се ресурси и ограничения;
- изисквания за управление на средата;
- изисквания за сигурност и безопасност и нива на класификация (евентуално и секретност);
- необходимите социални, икономически, технически и технологични условия;
- уточняване на терминологията;
- предложения.

III. ФАЗА НА ФОРМИРАНЕ (УСЪВЪРШЕНСТВАНЕ) НА РАБОТНИЯ ПРОГРАМЕН КОЛЕКТИВ

Едно от най-важните неща, което, за съжаление, често се пропуска или се анализира повърхностно, е нуждата от специфичен колективен подход за развитие на информационната среда. Факт е, че технически сръчности и умения се придобиват и в процеса на самата работа, но подход за работа, подход специфичен, творчески трябва да има априори „вътре“ в самия човек. Ударението, в този аспект, при развитието на технологичната информационна среда е необходимо да се постави на това, че хората в колектива трябва да са творчески личности, представители на различни научно-приложни дисциплини, свързани със съответната предметна област на средата. Работният програмен колектив трябва да се състои от специалисти от следните браншове:

1. Изследване на операциите. Това трябва да бъдат хора, способни да прилагат на практика класически и модерни математически методи.

2. Специалисти по проблемите на човешкото поведение (психолози). Тези специалисти са необходими за установяване и поддържане на оптимални връзки между останалите членове на колектива, а така също между хората и оборудването. Тяхна задача е да проучват и да се стремят да влияят на поведението на потребителите.

3. Софтуерни специалисти. Необходимостта от такива специалисти се проявява предимно при създаването (адаптацията) на различните информационни технологии.

4. Специалисти по информатика. Създават и прилагат критерии за оценка на софтуера, информационните технологии и оборудването. Осъществяват връзката между специалистите по изследване на операциите и всички специалисти от бранша „софтуер" относно приложението на определени методи или реализирани на тяхната основа процедури в рамките на една или друга информационна технология. Адаптират информационната среда към външните условия.

5. Статистици. Трябва най-рационално да се „употребяват" техните способности и талант да правят изводи и заключения на основата на определени съвкупности от данни и информация.

6. Проектанти на информационните фондове. Предлагат създаването на нови и изменението на съществуващите формати за съхранение на данните и информацията съобразно възможностите на софтуера, оборудването и другите специални ресурси и ограничения.

7. Висококвалифицирани специалисти по поддръжка на оборудването. Не е необходимо броят на тези специалисти да е голям. Достатъчно е те да бъдат най-много двама. Отричането на нуждата от такива специалисти и разчитането само на външни технически сервизи често водят до спъване, забавяне и разстройване на работата на цялата информационна среда. Трябва да се знае, че е необходимо програмният колектив да съдържа необходимия минимум от такива специалисти, защото доста често в процеса на работа на средата се налагат операции по инсталиране, замяна и усъвършенстване на оборудването в рамките на различните информационни технологии.

8. Методисти по обучението. Анализирайки „поведението" на информационната среда в процеса на нейното развитие и на основата на подходящо изграден учебен център (в рамките на организацията), да създават условия за развиващо и изпреварващо обучение както на членовете на колектива, така и на потребителите на средата. Тези специалисти трябва да са в постоянен контакт с най-изявените представители на научната, техническата и технологичната мисъл в областта на технологиите и технологичното развитие

и да намират и предлагат начини за рационално използване на техния потенциал.

9. Системни анализатори и проектанти. Тези специалисти трябва да притежават особени знания и сръчности по отношение на обработката на данни, информация и знания в специфичната област на технологичния трансфер. По принцип те трябва да са **технолози** с богат практически опит. Броят на тези специалисти зависи от обхвата и характера на предметната област.

10. Специалисти по управление. Задачата на тези специалисти е на първо място да предлагат ефективни и интелигентни управленски решения за рационалното развитие на информационната среда.

11. Специалисти по маркетинг. Това са специалисти с особени качества, които трябва да насочват своите усилия към осъществяването на ефективни търговски връзки с потребителите.

12. Административен персонал. Задачата на специалистите от този бранш е да осигуряват подходящи и нормални условия за работа на целия програмен колектив.

13. Ръководство на работния програмен колектив. Първото изискване към ръководството засяга неговия числен състав: броят на членовете му не трябва да превишава 8 – 10% от целия числен състав на колектива. Функциите на ръководството се свеждат главно до:

- следене, направляване и поддържане на развитието на информационната среда в съответствие с нейните цели и в рамките на поставената „социална поръчка“;
- вземане на решения относно целесъобразността на изразходваните средства.

14. Външни консултанти. Поради спецификите на предметната област на информационната среда е задължително непрекъснато да се контактува със специалисти, които имат големи знания и богат текущ практически опит в различни технологични направления. Ясни са съображенията, поради които тези специалисти не може, а и не трябва да бъдат постоянни членове на колектива. Задача на ръководството е да намери подходящи начини за тяхното привличане и финансово обезпечаване в съответствие с вложения от тях труд и на основата на съществуващите правни уредби.

IV. ФАЗА НА ПРЕДВАРИТЕЛНО ПРОЕКТИРАНЕ

Тази фаза е посветена изцяло на идентификацията, анализа и избора на главните проектни опции и алтернативи. На базата на предварителния анализ на всички процеси по входа, обработката и изхода на технологичната среда, извършен във фази I и II, тук се представят три типа възможности:

- операционни;
- технически;
- икономически.

Тези възможности се оформят във вид на доклад за вземане на съответни решения. Фазата на предварително проектиране не е свързана с правене на големи инвестиции. Отделните стъпки в тази фаза са:

1. Изготвяне на генерален модел за развитието на информационната среда.

2. Създаване на предварителни инструкции за ориентация по време на работата. Тези инструкции са първото приближение към новата или усъвършенстването на съществуващата системна документация на информационната среда.

3. Оформяне в окончателен вид на терминологичния речник.

4. Преглед на възможностите за разширяване на обсега на средата. Търсят се възможности информационната среда да се развива така, че в рамките на информационните ресурси да има възможност да „поема“ в бъдеще и допълнителни задачи.

5. Изготвяне на план за състоянието и развитието на трите компонента на информационната среда (информационни фондове, информационни технологии и взаимодействието човек – оборудване).

6. Идентифициране на операционните способности. Тази стъпка се отнася предимно за:

- комуникациите – брой и тип на автоматизираните работни места (ПК) които ще се поддържат в средата;
- мрежов или немрежов режим и пр.;
- информационни фондове – достъп;
- разпределени и неразпределени информационни ресурси;
- процесите on-Line или batch;

- в режим на времеделение или еднопрограмен режим и др.

7. Създаване на критерии за оценка и избор на функциите. Тук може да се използват следните съображения:

- средства за реализация;
- организационни изисквания;
- изисквания за контрол;
- секретност и безопасност на информационните фондове;
- изисквания, съобразени с желанията на потребителите;
- потенциални възможности за допълнително разширяване;
- настройваемост (адаптивност);
- наличен и достъпен софтуер;
- тип на софтуера (COMMERCIAL или IN-HOUSE);
- опит на членовете на колектива.

8. Избор на функциите.

9. Подробно диференцирано описание на функциите на оборудването и човешките функции в рамките на информационната среда (без реализация).

10. Развитие на изискванията за вход и изход. Тази стъпка резултира в следното: описание на всички входове и изходи, както на отделните компоненти, така и на цялата технологична среда.

11. Контролиране на цялостната конфигурация на информационната среда. От тази стъпка нататък трябва вече да е ясно, че сумата от отделните части дава не нещо друго, е желаната технологична информационна среда. Тук се създава т.нар. група за контрол на конфигурацията и всяка следваща (бъдеща) промяна на информационната среда трябва да минава за одобрение през тази група.

12. Избор на най-подходящата алтернатива за проектиране и развитие.

13. Планиране на текущото състояние на записите (records) на различните компоненти на информационните фондове.

14. Прецизиране на ограниченията на Средата.

15. Изготвяне на функционалната схема на Средата.

16. Създаване на план за инсталиране и развитие. Този план по същество трябва да се състои от две части:

а) разпределение на задачите по развитието на средата за целия период на новия жизнен цикъл; обикновено това разпределение се прави чрез т.нар. метод на критичните пътища (CPM);

б) персонално, текущо разпределение във времето на окрупнените конкретни задачи за всеки от периодите.

В резултат на това планиране се подготвят т.нар. таблици на относителната заетост (тези таблици се правят само за специалистите от колектива, които имат ключови позиции).

17. Създаване на план за текущо обучение на членовете на програмния колектив и потенциалните потребители.

18. Подготовка на икономическо изследване.

19. Подготовка на изследване за надеждност. Тази стъпка трябва да съдържа съображения относно: управлението, сигурността, секретността и достъпността до информационните фондове, текущото поддържане на средата, движението на информационните потоци, времевите ресурси и пр.

20. Подготовка на изследване относно поддръжката на информационната среда. Тук трябва да се засегнат въпросите, отнасящи се до усилията и необходимите ресурси, които се изискват за текущо поддържане на работоспособността на средата.

21. Изготвяне на доклад, представящ изпълнението на задачите през фазата на предварителното проектиране. Този доклад се представя за одобрение. Решенията, засягащи представения в доклада отчет и насоките за бъдещата работа, може да бъдат:

- да се продължи работата;
- да се извършат промени и отново да се представи за одобряване;
- да се отложи;
- да не се продължават усилията за развитие.

V. ФАЗА НА ДЕТАЙЛНО ПРОЕКТИРАНЕ И ТЕСТВАНЕ

Тази фаза започва след изчакване на съответното решение за директно продължаване на проекта или за извършване на изискваните корекции и модификации. Тук се проектират детайлно и се разработват входовете и изходите, типът организация и функционалното обвързване на информационните фондове и всички информационни технологии. Особено внимание се обръща на интеракцията човек – машина. Неразделна част от тази фаза е и създаването на необходимата системна документация (първи вариант).

Тестване се извършва още на фазата на предварителното проектиране, но там то не е цялостно, а на някои отделни функцио-

нални части на Средата. Тук тези части вече са обединени и тестването покрива цялостната работа на информационната среда.

При фазата на детайлното проектиране и тестване е необходимо да се оформят две функционално обособени групи от членовете на колектива. Едната е възможно да се нарече група за проектиране на оборудването, която ще проектира и реализира логиката на предимно машинните функции, а другата – група за проектиране и реализация на „човешката част" от технологичната информационна среда.

Отделните дейности, които е необходимо да се извършат през тази фаза, може да се реализират в следните стъпки:

1. Установяване на позициите. Един от резултатите от тази стъпка е оформянето на общ поглед върху състоянието на информационната среда (ако съществува такава) и/или анализ на направеното в предишните фази, за да се установи дали всичко необходимо за детайлното проектиране е налице. Друг съществен резултат е изготвянето на т.нар. позиционни диаграми. Чрез тези диаграми се индикират последователността на изпълнение и връзките между отделните задачи.

2. Подготовка на инструкции за работа. На основата на разработените в предходната фаза таблици на относителната заетост се подготвят пакети от инструкции за всеки от членовете на колектива, в които се установяват съвкупността от задачите за изпълнение и други допълнителни персонални изисквания.

3. Окончателно проектиране на функционално-логическата структура на информационната среда.

4. Определяне на софтуера. Тази стъпка засяга окончателния избор на операционните системи (ОС), езиците за програмиране, мрежовия софтуер и др.

5. Определяне на начините за вътрешноексплоатационно описание на постъпващата информация. Трябва да се изготвя матрица, в която да са отбелязани типът на различните информационни източници и съответните инструкции за описание на информационния вход, съответстващ на всеки от тези източници.

6. Изграждане на логическата структура на информационните фондове. Обикновено поради спецификата на технологичната информация информационните фондове тук се разделят на два вида – основни, които ще бъдат върху магнитни носители, и

поддържащи, които ще се съхраняват на хартиени носители.

7. Установяване на изисквания за необходимия интерфейс. Развитие на интерфейсните процедури.

8. Детайлно описание на всички възможни интеракции между човека и оборудването в рамките на технологичната информационна среда. Това описание включва развитието на методи, които да отчитат специфичната роля на човека по време на работа.

За първи път проблемите на човешкия фактор в процеса на взаимодействие с машините стават предмет на задълбочени научно-приложни изследвания през 1940 г. в лабораториите на телефонната компания „Бел“ в САЩ във връзка с проектирането, разработването и внедряването на система за далечно избиране за нуждите на армията. Тогава се поставят основите на една от бурно развиващите се съвременни научни дисциплини – **Human Factor Engineering.** Най-често областите на проявление на тази дисциплина са свързани с изследвания и изучаване на:

- сензорни способности;
- моторни сръчности;
- вземане на инцидентни решения в условията на минимална информационна наситеност;
- групови комуникации;
- работното място и неговата среда;
- условията за възникване на стрес, умора и пр. и начините за тяхното преодоляване.

При проектирането и реализацията на входовете и изходите на информационната среда трябва да се обърне внимание на формата на показване на информацията върху дисплеите. Тази форма трябва да е съобразена със следните условия:

- време за търсене;
- информационно съдържание;
- код на представяне;
- интензивност на дисплея;
- размер (максимално количество информация, изобразено на един екран);
- методи за представяне и др.

Особено важно е да се разбере, че **Human Factor Engineering** не е „кръпка“ към информационната среда, а неразделна част от нея.

9. Описание на изисквания за ефективно администриране на средата.

10. Описание на изисквания за безопасност и цялостност на информационните фондове.

11. Развитие на изискванията за надеждност.

12. Идентифициране и уточняване на нуждите от входно-изходни устройства.

13. Идентифициране и уточняване на изискванията към централния процесор.

14. Идентифициране и уточняване на изискванията към останалото оборудване.

15. Окончателен избор на хардуера и софтуера.

16. Проектиране и създаване на операционните форми. Това са формите, които ще се подават и извеждат на екраните на терминалите (персоналните компютри) – менюта, командни диалози и пр. Тези форми трябва да са съобразени с изискванията, предявени в стъпка 8.

Съществуват няколко метода за проектиране и реализация на операционните форми:

а) Метод на филтриране – при този метод информацията се редуцира само до това, което действително ще е нужно на потребителите; филтрация се извършва поотделно за всеки потребител съобразно неговите характеристики;

б) Метод на ключово представяне – тук в зависимост от целите на потребителите се предоставя информация само за т.нар. ключови променливи на изследваните обекти, като например:

- за хората – ключови променливи са критичните диагностични фактори: пулс, кръвно налягане, температура и пр.;
- за автомобилите – ключови променливи са: състояние на цилиндрите, свещите, гумите, спирачките, предавките и пр.;

в) Мониторинг метод – това е също метод, на чиято основа се редуцира количеството на информацията, представяна в отделните операционни форми; има два основни пътя за приложение на този метод:

- вариантно представяне – тук се изисква информацията за няколко събития да бъде сравнявана предварително с еталон и само тази информация, при която „разстоянието“ до еталона е най-малко, да се предоставя на потребителите;

• автоматични съобщения – създават се определени операционни форми за автоматично извеждане на информацията (например възможно е всеки ден автоматично да се получават диференцирани списъци на новите постъпления в информационните фондове на технологичната среда);

г) Метод на моделирането – при този метод се използват логико-математически модели за трансформиране на информацията в подходящи за конкретните потребители операционни форми. Моделите може да се настройват както от отговорния за това персонал на Средата, така и от самите потребители. В този случай тези модели се делят по следните критерии:

• според функциите:

– дескриптивни – дават проста картина на ситуацията, без да препоръчват никакви действия;

– предикатни – индикират, че ако нещо се случи, ще следва...;

– нормативни – дават „най-добрия“ отговор; препоръчват поредица от действия;

• според структурата:

– иконични – базират се на физическите структурни характеристики на представените същности;

– аналогови – при тях съществува субституция между компонентите и процесите;

– символни – използват символи (символни единици) за описание на проблема;

• според времето:

– статични – не отчитат промяната на времето;

– динамични – при тях времето е независима променлива;

• според степента на несигурност:

– детерминирани – дават решение на модела само при сигурни условия;

– вероятности – дават решение на модела при условие на риск;

– игрови – използват теорията на игровото моделиране, за да търсят оптимално решение;

• според общността:

– общи – прилагат се за няколко близки функционални области;

– специализирани – прилагат се само за уникални проблеми.

17. Проектиране и изграждане на информационните фон-

дове (с експериментални данни). Описание на всички логически информационни елементи.

18. Проектиране и изграждане на информационни технологии както в рамките на отделните компоненти, така и в Средата като цяло.

19. Проектиране и изграждане на помощни модули.

20. Подготовка на план за тестване (евентуално и верификация).

21. Написване на първи вариант на системната документация.

Обикновено тестването е доста травмиращ процес. Това е така, защото почти винаги до неговото започване не се знае какви ще бъдат критериите за това. Тестването не бива да бъде отделна фаза, а да се вписва изцяло във фазата на детайлното проектиране. Продължавайки поредицата от стъпки в тази фаза, следващите такива ще бъдат:

22. Формиране на група за тестване. Задължително в тази група се включват и представители на потенциалните потребители.

23. Тестване на логиката на информационната среда.

24. Тестване на основните и спомагателните трансакции.

25. Тотален тест. Тази стъпка трябва да се раздели на две части:

- тестване на работоспособността на системата с реални данни;
- тестване на възможностите за възстановяване както на всяка процедура в рамките на различните информационни технологии, така и на информационните фондове и Средата като цяло.

26. Проверка на съответствието на системната документация с работата на технологичната информационна среда в реални условия. В резултат на тази стъпка евентуално системната документация може да се коригира, след което тя вече добива окончателен вид (първи вариант).

27. Разпределение (преразпределение) на функциите на организационните звена в рамките на организацията, отговаряща за развитието на технологичната информационна среда. Тази стъпка подсказва, че в съответствие с цикличността на работата по развитието на средата периодично се налагат и организационни промени, отговарящи на новите условия за нейното съществуване и развитие.

28. Изготвяне на доклад за изпълнението на фазата,

„придружен“ от работоспособна „версия“ на информационната среда, с необходимата документация.

VI. ОРГАНИЗАЦИЯ И АНАЛИЗ НА ПРОЦЕСИТЕ ПО СЪБИРАНЕТО НА ТЕХНОЛОГИЧНА ИНФОРМАЦИЯ

Една от основните, а може да се каже, и главната функция на технологичната информационна среда (а и на всяка информационна среда) е да предлага на потенциалните потребители достатъчна по количество и с добро качество технологична информация. Но за да се предостави на потребителите, тази информация трябва да се събере. Известна истина е, че каквото се „вкара“ в информационните фондове, в крайна сметка това и ще се „изкара“. Ето защо от тази фаза в голяма степен зависи качеството на информационната среда.

Процесите по събиране на технологична информация може да се разделят на шест главни етапа:

1. Установяване на изискванията за типа, вида и количеството на необходимата технологична информация;
2. Определяне на периодичността на „доставката“ на информацията;
3. Определяне на главните информационни източници;
4. Събиране на необходимата информация;
5. Анализ и оценка на информацията;
6. Попълване на информационните фондове на Средата.

Що се отнася до наименованията, то тези етапи са едни и същи независимо от характера на информационната среда. При разглеждането обаче на тяхната същност в контекста на информационната среда ясно се вижда, че те носят спецификата, характерна само за тази предметна област. Лесно е да се каже например, че начините за събиране на данни и информация са следните:

- чрез въпросници;
- чрез интервю;
- от фирмена литература;
- от специализирани бази данни и други информационни фондове, и пр.

Достатъчно е обаче да добавим думата „технологични“ пред словосъчетанието „данни и информация“ и ситуацията вече коренно се променя. Който практически не се е сблъсквал с пробле-

мите, засягащи процесите по събирането на технологична информация, надали може да си изгради ясна представа за реалните трудности, съпътстващи тези процеси. Типичен пример в това отношение е Информационният център за трансфер на технологии ИНФОРМА, България, който премина по пътя, водещ от етапа на купуването на технологична информация от непосредствените и първични създатели към етапа на заплащане от страна на същите тези създатели, щото именно тяхната технологична информация да бъде „вкарана" във фондовете на ИНФОРМА.

Съществуват много подходи за организация на процесите по събиране на технологична информация, но всички те може да се обобщят в три основни, определящи всъщност и типа на организациите, които са отговорни за съществуването и развитието на информационната среда:

1. Изграждане на централизирани национални технологични информационни фондове. При този подход се създават специални организации или се оторизират съществуващи такива да бъдат фондодържатели и фондоразпространители на технологична информация с национално значение. Дейността на тези организации се определя с правителствени разпоредби. Трябва да се обърне внимание на обстоятелството, че базирайки се на огромното социално въздействие на технологичната информация, всяка страна, претендираща за челни позиции в научно-техническия прогрес, има изграден централизиран технологичен фонд (пример е NTIS, САЩ). Погрешно е схващането, че управлението на този фонд е част от централизираното управление на научно-техническите[10] информационни ресурси. Спецификата на създаването, поддържането, разпространението и използването на технологичните информационни ресурси изисква и налага тяхното самостоятелно управление и контрол.

Механизмът на създаване на централизиран национален технологичен фонд е следният:

- Правителството чрез различните си институции отпуска средства и възлага изпълнението на проекти или закупуването на готови технологични решения на отделни организации;
- При етапното или окончателното отчитане на резултатите от изпълнението на тези проекти или след внедряване на готовите технологични решения организациите изпълнители или органи-

зациите, оторизирани да закупят технологичните решения, задължително предават описаната в специален формат технологична информация за оценка, анализ, допълнителна обработка, съхранение и разпространение в централизирания национален технологичен информационен фонд;

• Правителството финансира националния технологичен информационен фонд както за организирането на процесите по събиране, съхраняване и разпространение на технологична информация, така и за закупуването на информация от чужди информационни институти. То също упражнява контрол върху цялостната дейност на националния технологичен информационен фонд.

2. Създаване (възникване) на специализирани информационни центрове. Този подход е както количествено, така и качествено допълнение на описания по-горе първи основен подход. Концепцията за създаване на информационни центрове в никакъв случай не противоречи на създаването (наличието) на национален технологичен информационен фонд. Тези специализирани организации трябва да бъдат притегателни центрове за всички създатели или ползватели на едни или други специфични технологии и технологични решения. След съответно заплащане от тяхна страна информацията на създателите на технологии се прибавя (анализира, оценява, допълва) към технологичния информационен фонд на съответния информационен център, а потенциалните потребители на фонда купуват[11] анализираната и преработена технологична информация и технологични знания (например „Дворкович", САЩ, ИНФОРМА, България). Този процес е сравним с процеса на поместване на рекламно обявление във вестник.[12] За да бъде отпечатано, „собственикът" **А** на обявлението заплаща дадена сума на „собственика" на вестника. След излизането на вестника той се продава и съответно купува за определена сравнително малка сума. Един от възможните купувачи може да бъде и собственикът **А**. Ясно е, че в такъв вестник може да се публикуват рекламни обявления от много други собственици: **Б, В, Г**, ... Купувайки вестника, собственикът **А** има потенциалната възможност наред с информацията от общ характер (която в общия случай е полезна за него) да се запознае и с обявленията на собствениците **Б, В, Г** и пр. Възможно е някои от тези обявления плюс информацията от общ характер да бъдат толкова полезни за собственика **А**, че многократно да покрият неговите разходи както

за поместването на обявлението, така и за купуването на вестника. Това се отнася и за всички други собственици: **Б, В, Г** и пр.

3. Смесен подход. При този подход чрез определени неголеми финансови инвестиции и правни уредби държавата (правителството), от една страна, контролира изпълнението на социалните функции на даден информационен център (за трансфер на технологии), в който се съсредоточава националният технологичен информационен фонд (НТИФ), а от друга, дава възможност и насърчава този център да развива своята дейност в съответствие с втория основен подход.

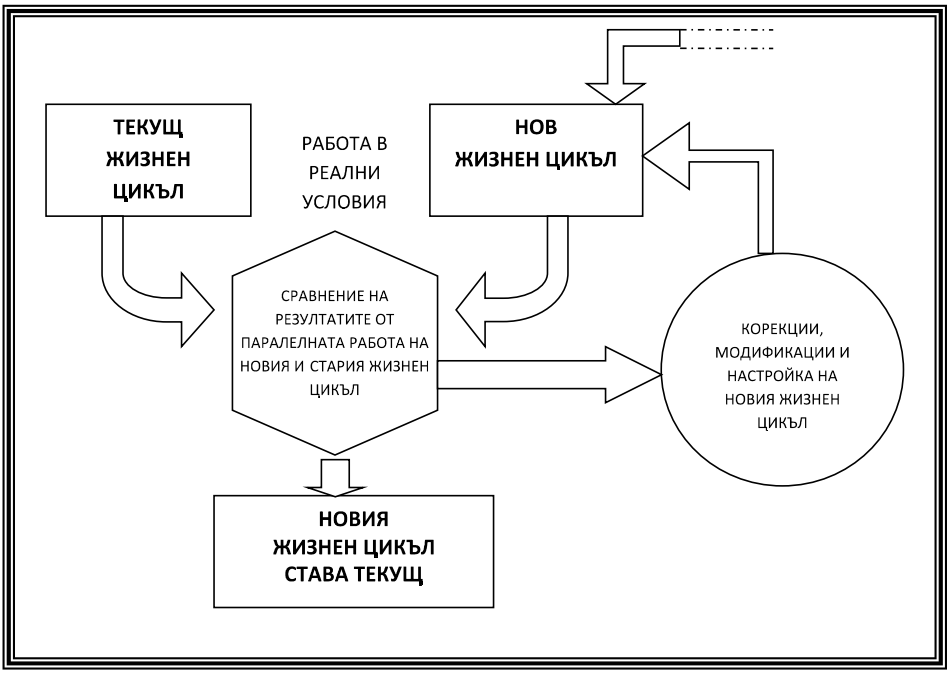
Характерна особеност на процесите по събиране на технологична информация е и тази, че за разлика от много други типове информация „произвеждането" ѝ не се извършва в рамките на специализираната организация, отговорна за развитието на информационната среда за трансфер на технологии, а идва там вече „произведена". Може да се каже, че в 90% от случаите на входа на технологичната информационна среда постъпват не технологични данни, а технологична информация. Това от своя страна е предпоставка за активен контакт (включващ и обучение) с първичните създатели и внедрители на технологии и технологични решения с цел обезпечаване на условия, така щото подготвяната от тях информация да бъде годна за използване. Независимо от това, че на входа на средата постъпва „готова" технологична информация, тази информация до „вкарването" си в технологичните информационни фондове минава през няколко етапа на анализиране и предварителна оценка:

- верификация и класификация – по определена методика се проверява верността ѝ и се извършва диференциация по определени критерии;
- ранжировка/сортиране – информацията се подрежда на основата на предварително зададена наредба;
- логически манипулации – извършват се редуциране и подреждане на информацията по определени логически критерии;
- математически манипулации – извършват се математически операции с информацията;
- репродуциране – дублиране на информацията върху носители от един и същ тип или върху разнотипни носители с цел надеждно и безопасно съхраняване; и др.

VII. ВНЕДРЯВАНЕ (ЗАМЯНА)

Както тестването (което в общия случай е недостатъчно) тази фаза също е травмиращ процес. Това е така, защото тук се изглаждат последните „дефекти“ от развитието на технологичната информационна среда, след което този жизнен цикъл на Средата се смята вече за работоспособен.

Внедряването (замяната) се извършва, когато новият жизнен цикъл на информационната среда започва да замества стария, оперирайки активно и паралелно с него. Този процес е показан на фиг. 3.



Фиг. 3. *Фаза на внедряване (замяна)*

Формалният край на тази фаза настъпва, когато „новата“ информационна среда се „приеме“ напълно от потребителите на технологична информация и технологични знания, след извършването на евентуално исканите от тях промени (в съответствие с предварителните договорености) и корекции, наложили се в резултат от допуснати грешки и отклонения от проекта.

VIII. ОПЕРАЦИОННА ФАЗА. ЕКСПЛОАТАЦИЯ

В периода на един жизнен цикъл на информационната среда тази фаза е с най-голямо значение. Това значение се определя както от продължителността на фазата, така и от обстоятелството, че именно тук Средата дава своите реални резултати. Началната точка на операционната фаза се поставя непосредствено след фазата на внедряването и паралелно с процесите по събирането на технологична информация. По-късно, по време на развитието на тази фаза, събирането на технологична информация става един-единствен неин компонент. Експлоатационната фаза формално завършва, след като се прецени, че е необходимо да се замени, модифицира (нов жизнен цикъл) или преустанови работата на текущата технологична информационна среда.

IX. КОНТРОЛ, ПОДДРЪЖКА И ИЗДРЪЖКА НА ИНФОРМАЦИОННА СРЕДА

В процеса на експлоатационната фаза се извършват специфични дейности по поддръжката и контрола на информационната среда. Целта на тази поддръжка и контрол е запазването (подобряването) на ефективността от работата за планирания период от експлоатацията на информационната среда. Дейностите по поддръжката се асоциират с:

- поддържане на средата в постоянна изправност;
- редовно и бързо отстраняване на възникващите аварийни ситуации;
- замяна на морално и физически остарели елементи на средата;
- текущо сервизиране.

От изключително важно значение за работата на информационната технологична среда са дейностите на нейния текущ контрол в процеса на експлоатацията. Тези дейности може да се диференцират по следния начин:

1. Входящ контрол. Тук постоянно се контролират:

- кодовете на трансакциите за достъп до средата;
- входните форми и формати – видът им и наличието на необходимите атрибути;
- съдържанието, същността на технологичната информация – верификация, по модул 11 и други подобни техники, визуално, чрез средствата на изкуствения интелект.

2. Програмен контрол:

• периодично тестване и верификация на програмното осигуряване;

• установяване на различни ограничения при логическите и аритметичните операции върху технологичната информация;

• аритметични „доказателства“ – например, ако се борави с ценова информация и общата стойност е 10 000, а изразходването е 7000, ясно е, че това, което остава, трябва да е 3000;

• поддържане на дневник на грешките;

• поддържане на дневник на трансакциите.

3. Контрол на информационните фондове:

• физически контрол – периодична проверка на физическото състояние на носителите на информация и осигуряване на условия за контролираното им съхраняване;

• логически контрол – извършва се чрез „пускането“ на специални програми, които трябва да дадат очаквани в някакви граници резултати;

• процедурен контрол – опира до наличието на специален персонаж, отговорен за поддръжката на информационните фондове; винаги трябва да се съхраняват актуални копия на информационните фондове на три нива: „дядо – баща – син“.

4. Изходящ контрол:

• екранното визуализиране трябва да дава възможност за индициране на грешна информация;

• всички неинтерактивни изходни форми трябва да се разпределят от специално оторизирано лице;

• да се намерят форма и средство да се изисква от потребителите да съобщават за евентуални грешки в работата на Средата независимо от техния характер и големина.

5. Контрол на документацията. Този контрол се извършва главно по сигнал на потребителите и чрез специално назначени „ревизори“. Документацията трябва да е разделена на три основни типа:

• обща документация за информационната среда;

• процедурна документация;

• програмна документация.

Като пример контролните изисквания към документацията от последния тип са следните:

• документацията трябва да е направена описателно, като се следва дадената още в началото функционална схема на технологичната информационна среда;

• трябва да съществува диференциация на входовете, изходите, обработката и другите специални програмни модули;

• да съдържа JCL с изрично обяснение на всяка команда;

• всички добавени модули трябва задължително да се описват;

• листингите с началните и обектните кодове трябва задължително да са включени в документацията;

• за всеки програмен модул трябва да има относително прости, подробно описани примери;

• изрично трябва да са описани всички контролни точки на програмите;

• наложително е наличието на всички потребителски (и ако има такива – операторски) инструкции и съобщения заедно с обясненията на съответните действия;

• отделно трябва да се съхранява дневник за текущото състояние на програмните модули.

6. Контрол на оборудването:

• задължително при доставката трябва да се изисква фирмен контрол, придружен със съответните сертификати за гаранции;

• контрол през периода на инсталирането;

• текущ сервизен контрол.

7. Операционен контрол на условията на експлоатация:

а) физически контрол:

• контрол на мястото;

• контрол на условията – температура, влажност, силова токова система, прах и др.;

б) процедурен контрол. Този тип контрол „следи“ за стриктното изпълнение на процедурите по режима на работа (отворен или затворен режим, режим на времеделене, поддържане на необходимите условия за работа в терминални или компютърни зали и пр.).

8. Контрол за безопасност и секретност

Този контрол е комбинация от методи и средства, които дават възможност да се запази целостта на информационната среда и в частност на информационните фондове от случайни грешки в оборудването, софтуера, от грешки, предизвикани от хората, или пък да се предпази средата от неоторизиран достъп. По-важните рискови фактори тук са:

а) човешка грешка – „малка“ волна или неволна грешка на човек може да доведе до големи загуби;

б) измама и неоторизиран достъп:

в) индустриален шпионаж;

г) копиране на информация от телекомуникационните линии чрез средствата на on-line достъпа;

д) физическа кражба на информационни носители;

е) инсталиране на програми „вируси“;

ж) саботаж;

з) физически повреди в захранването с електричество или в комуникационните линии;

и) пожар;

й) непредотвратими природни бедствия – наводнения, земетресения, пожари, урагани и др.

Изброените по-горе фактори определят и целите на противорисковия контрол, а именно:

а) на първо място – предотвратяване на произшествието;

б) своевременна индикация на нарушенията на нормалната работа на информационната среда и „уведомяване“ на оборудването и отговорните за това хора с цел предприемане на коректривни действия;

в) минимизиране на отрицателното въздействие от евентуални загуби;

г) пълно разследване на всяка неконтролирана рискова операция;

д) възстановяване на загубите.

9. Техника за физическо осигуряване

а) контролиране на достъпа:

- осигуряване (ако е необходимо) на пазачи и специални придружители;
- регистриране при влизане и излизане;
- използване на цветни кодове (сложени на видно място) за различните категории персонал и за потребителите;
- контролни карти;
- използване на вградени телевизионни камери и монитори;

б) контрол на мястото:

- мястото, където е разположено основното компютърно оборудване на Средата, трябва да е далеч от радарни и микровълнови

инсталации, магнитно-силови установки и др., на разстояние, повече от 500 м;

в) физическа защита:

- осигуряване на противопожарен контрол;
- осигуряване на контрол на входните инсталации.

10. Техники за процедурно осигуряване

По принцип е трудно да се направи рязко разграничаване между физическото и процедурното осигуряване, защото те в много случаи се припокриват, но все пак може да се посочат основните моменти, на които трябва да се обърне внимание тук:

а) цялостност – информационната среда трябва постоянно да бъде поддържана в пълна комплектност и функционална коректност;

б) изолация – ако е необходимо, трябва да се осигурят:

- географско или логическо отделяне на определени структурно и функционално отделени елементи на средата;
- разстановката на терминалите (персоналните компютри) за достъп да бъде на нива; ако ще се ползва информация с елементи на секретност, съответното оборудване за достъп трябва да бъде надеждно изолирано; принципно съображение е броят на хората с привилегирован достъп до информационните фондове да бъде сведен до минимум;

в) идентифициране – възможно е да се използват следните „техники“:

- потребителски атрибути за достъп – магнитни карти, ключове и др.;
- потребителски характеристики – геометрия на тялото, глас, подписи, отпечатъци от пръстите и устните, ирис на ретината на окото и др.;
- авторизация – обикновено тук се извършва категоризация на потребителите;

г) мониторинг – осигуряване на условия за:

- автоматично разпознаване на различни рискови фактори;
- изключване на съответното оборудване (например при n-ти опит за неоторизиран достъп) и уведомяване на отговорния персонал;
- запис на всички нарушения или съмнения за нарушение на установения режим (в информационната среда трябва да се съдържат данни за всички потребители).

Важна дейност, осъществявана в процеса на развитието на ин-

формационната среда, е дейността на нейната издръжка. Много често при анализите на подобни същности тази дейност съзнателно или несъзнателно се пропуска. Това пропускане обаче в общия случай се отразява неблагоприятно върху цялостната работа и често води до непоправими последствия.

Дейностите по издръжката на информационната среда са в пряка връзка и непосредствена зависимост от типа на организационните структури.

X. ТЕКУЩ АНАЛИЗ И ОЦЕНКА НА СЪСТОЯНИЕТО НА ИНФОРМАЦИОННА СРЕДА

Веднага след замяната на текущия (стария) жизнен цикъл на Средата с разработения нов такъв отново започва процесът на анализ и оценка на състоянието на действащата технологична информационна среда. На основата на резултатите от този анализ се извършват едни или други корективни действия, целящи подобряване на резултатността и ефективността от работата ѝ. В много случаи системното извършване на анализ на състоянието на информационната среда спомага съществено за удължаване на текущия жизнен цикъл, без това да се отрази на работоспособността на Средата.

В резултат на текущия анализ и оценката на състоянието е възможно да се вземат пет различни вида решения:

1. Извършване на промени в информационната среда, целящи запазване или подобряване на работоспособността ѝ;

2. Модификация на външните условия, в които средата съществува и се развива;

3. Започване на работа по създаване и развитие на нов жизнен цикъл;

4. Замяна на текущия с нов жизнен цикъл;

5. Прекратяване на работата на информационната среда. Обикновено решение от такъв тип се взема при извършване на коренни промени в структурата на отговорната за информационната среда организация.

РАЗВИТИЕ НА СРЕДА ЗА ИНФОРМИРАНЕ

Тук ще обърнем внимание на процеса на информиране, като разгледаме основните етапи от гледна точка на усвояването и използването на информацията. Специално внимание ще отделим на гаранциите за осигуряване на успех в процеса на информиране.

Общи положения

При процеса на информиране имаме двама участници – изпращач и получател. Изпращачът иска да съобщи на получателя определено съдържание. За целта той формулира съобщение, в което кодира исканото съдържание според своето разбиране, експертност, култура. Съобщението се кодира в зависимост от средата или канала за пренос в сигнал, който се транспортира до получателя. При получателя сигналът се декодира, като се възстановява оригиналното съобщение. Следващите фази определят дали съобщението е разбрано, прието и доколко формира у получателя знание, което тя/той ще използва при вземане на решения или по-общо – при определяне на своето поведение. В този процес може да разграничим три етапа: формулиране на съобщение, пренос, интерпретация и формиране на знание. Вторият от тези етапи – преносът, включва кодиране – транспортиране – декодиране и е от интерес за изучаващите техническите характеристики на различните медии, използвани за пренос на данни.

При класическите комуникационни теории се приема, че задачата е решена, ако съобщението е декодирано коректно. Етапите на интерпретиране, приемане и прилагане обаче са от съществено значение за постигането на целта – информиране на потребителя. Рисковете при постигането на целите на процеса на информиране са както при преноса на сигнала, породени от шум в канала за пренос (тук с „шум“ ще бележим всички външни въздействия, които изкривяват сигнала при неговото транспортиране), така и при неразбиране, грешно интерпретиране или отхвърляне на информацията поради недоверие. В тези случаи се генерира грешно знание, което може да доведе до грешни действия, или не се генерира знание, тъй като получената информация се игнорира (не се приема) и не поражда действия. След като получателят разбере и интерпретира получената информация, ако той има доверие в нея, т.е има

основание да я приеме за надеждна и правдоподобна, тогава тя е ценна за него и той ще я използва за вземане на решения.

В случай че информацията, предназначена за получателя, противоречи на неговите възгледи и преценка за проблема, то процесът на информиране се оказва неуспешен, т.е. информирането води до увеличаване на несигурността по отношение на поведението на получателя и е много вероятно да бъде отхвърлена. Погрешното разбиране, интерпретиране на съобщението води до грешни решения (предполагаме, че съобщението съдържа коректна информация) и действия; потребителят е заблуден от съобщението. С такава ситуация се свързва понятието „мисинформация" – изпращачът предава коректно съобщение, което обаче води до заблуждаване на получателя.

Източници на риск за неуспех при процеса на информиране може да има в различните етапи на комуникационния процес вследствие на:

1. Формулиране на съобщението по неподходящ начин от източника на информация;

2. Външни фактори, които изкривяват информацията (от физическата среда на процеса);

3. Кодиране/декодиране на съобщението, което в някаква степен може да измени смисъла на предаваната информация;

4. Интерпретацията на съобщението от получателя на информация, повлияна от информационната асиметрия, може да доведе до различно тълкуване.

Трябва да се отбележи, че всички етапи на процеса на комуникация са еднакво важни, защото, ако някой от етапите е неуспешен, това означава, че целият процес е неуспешен.

Следната йерархия на цели описва сложността на този процес и дефинира понятието **„качество на информиране"** (D. **Christozov**, **Chukova**, S., **Mateev**, P. Informing Processes, Risks, Evaluation of the Risk of Misinforming. – In: **Gill**, G., E. **Cohen** (editors). Foundation of Informing Science: 1999 – 2008. Informing Science Press, 2009, pp. 223 – 356):

Дефиниция: Под „качество на информиране" ще разбираме информационен процес, който:

1. ниво – гарантира коректно пренасяне на съобщението от изпращача до получателя, т.е. декодираното съобщение е идентично с оригиналното;

2. ниво – гарантира, че съобщението е прочетено и разбрано от получателя. Тук се третират два типа рискови събития – езикът, на който е съставено съобщението, е непознат на получателя, и терминологията, използвана в съобщението, е непозната на получателя. И в двата случая съобщението не може да бъде разбрано и следователно не информира получателя;

3. ниво – гарантира, че получената информация ще бъде приета от получателя и ще послужи за генериране на ново знание. Тук трябва да бъде решаван въпросът за степента на доверие към източника и към съобщението. Рискът е от отхвърляне на информацията;

4. ниво – гарантира, че новото знание, генерирано в резултат на получената информация, съвпада със знанието, което изпращачът е искал да предаде. Успехът на това ниво също показва, че намеренията на изпращача съвпадат с потребностите на получателя.

На практика при класическите информационни системи акцентът пада върху първите две нива. Въпросът за факторите, влияещи на доверието към получената информация, е въпрос, отговорът на който затваря кръга на цялостния процес на информиране.

Осигуряване на доверие

В литературата (**Gackowski**, Z. Quality of Informing: Credibility – A provisional model of functional dependences. – In: *Informing Science: The International Journal of Emerging Transdiscipline*, 9, 2006, pp. 225 – 241; **Gackowski**, Z. A formal Definition of Operation Quality of Factors – A Focus on Data and Information. – In: *International Journal of Information Quality*, 1(2), 2007, pp. 225 – 249) се използват различни понятия, като „надеждност“ (reliability), „вяра“ (believability), „доверие“ (credibility), за да се обозначи доколко адресатът приема и вярва на получената от даден източник информация. Най-често се използва понятието „доверие“ (credibility) като атрибут, характеризиращ качеството на получените данни/информация/знания. Доверието е много важна характеристика на информацията в процеса на вземане на решения.

Доверие – означава дали и доколко адресатът приема, че получената информация е вярна, дали тя не противоречи на неговото мнение, вяра и/или знания и очаквания. Доверието е мярка за това дали потребителят може да разчита на получената информация при формирането на поведение.

Стопроцентово доверие е практически невъзможно. Съществува някаква граница – праг (actionable credibility), която е степента на доверие към получената информация, при която лицето, вземащо решение, е склонно да пристъпи към действие (вземане на решение) на базата на получената информация.

Най-често доверието по отношение на валидността или верността на информацията е функция от репутацията на източника на информация. Всяка информация наследява доверието, което имаме в съответния източник, от който я получаваме.

Осигуряване на доверие по първични фактори

Основните фактори, влияещи директно върху степента на доверие, което имаме към получената информация, са:

- репутацията на източника на информация;
- разнообразието и количеството независими алтернативни източници на информация – ако няколко независими конкурентни източника потвърждават една и съща информация, това значително увеличава степента на доверие към нея.

Източниците на данни или информация може да бъдат различни наблюдатели, сензори, процеси, анализи и т.н. Някои от тях дори не може да бъдат идентифицирани от получателя на информацията. Други той получава от известни, използвани от него вече източници с добра репутация и това увеличава степента на доверие в тях.

Всяка информация, получена от даден източник, наследява доверието, което имаме в него. Следователно доверието в дадена информация може да определим като специфично доверие, съгласно произхода ѝ. Ако има допълнителни алтернативни източници, с които да се съпостави добитата информация, несигурността намалява. Ако от много източници се получи еднаква или подобна информация, то съвместното доверие **(joint credibility – JC)** се явява допълнение към произведението на допълненията на доверието към всеки отделен източник:

$$(1 - JC) = \prod_j (1 - C_j),$$

където с C_j бележим доверието към даден източник, измерено в интервала (0,1).

Информацията, която потребителят получава от източника, трябва да бъде:

- пълна;

- ясна/недвусмислена;
- смислена;
- коректна.

В същото време, за да може получателят да я интерпретира правилно, тя трябва да му бъде представена по подходящ начин, така че да бъде разбираема за него (на разбираем за него език, в предпочитани от него измервателни единици и т.н.), което определя риска от погрешно разбиране на предаваната информация, т.е. риска от мисинформиране. Това прави представянето на информацията (presentation credibility) много важен фактор за осигуряване на доверие.

Осигуряване на доверие по вторични фактори

Освен първичните фактори за осигуряване на доверие задължително трябва да се разгледат и вторични фактори, които също играят съществена роля при окуражаването на потребителя да използва предоставената информация:

- Проследимост (traceability). Възможността за проследяване на източниците на информацията е много важна предпоставка, която дава възможност на получателя на информацията да идентифицира първичните източници, за да формира доверие към предоставените данни;
- Наличие на надежден комуникационен канал. Наличието на надеждна комуникация между източника и получателя на информация е необходима предпоставка, за да се гарантира на получателя, че съобщението не е променено в процеса на комуникация;
- Конфликт на отношения и интереси (alignment attitudes and interests). При процес на активно информиране много важно е отношението между страните. Ако по някакъв начин източникът на информация е заинтересован от действията на получателя на информация и особено ако има конфликт на интереси, доверието в този източник рязко пада;
- Надеждност (reliability) – в смисъл на репутация на източника на информация;
- Възможност за проверка на репутацията (verifiability). Съществуват различни форми за проверка на репутацията на източниците. Една от тях е периодичната акредитация на източника от някаква известна независима институция (trusted third party), коя-

то удостоверява неговия статут и повишава доверието в него. Друга форма е предоставянето на възможност за запознаване и ревизия на процеса, довел до създаване и предоставяне на информацията;

• Повторяемост на информацията (replicability). Това е друга форма на подсигуряване на клиента, когато източникът на информация дава възможност да бъдат възпроизведени и повторени определени действия, довели до създаването на предоставената информация. Тази форма е приложима при предоставяне на вторична информация, информация, продукт на осъществена обработка и анализ на първичните данни. Повторната обработка, с евентуално включване на нови аналитични техники, цели потвърждаване на получените изводи;

• Даване на гаранция (warranty). Гаранцията, като елемент на договора между страните, е друг инструмент за повишаване на репутацията на източника на информация от гледна точка на клиента. Чрез споделяне на риска от страна на източника на информация значително се увеличава доверието в него. Наличието и големината на гаранцията са индикация за това доколко се намалява рискът за потребителя на информация, който в този случай може да бъде разглеждан като клиент на изпращача в случай на дефекти в качеството на информацията.

Последните четири фактора: надеждност, възможност за проверка на репутацията, повторяемост на информацията и гаранции, служат за повишаване на репутацията на източника и доверието в него и може да бъдат разглеждани като инструменти за управление на процеса на информиране. В тази глава е изследван основно факторът гаранции.

От друга страна, обратен ефект имат всички нарушения по отношение на:

- дефинирането;
- обективността;
- променливостта;
- точността;
- прецизността;
- актуалността на информацията.

Те спомагат за неправилното представяне на информацията, което съответно увеличава риска от погрешното ѝ интерпретиране и намалява доверието в нея (presentation credibility). Това оказва негативно влияние върху репутацията на източника на информация.

НАУКА ЗА ИНФОРМИРАНЕТО

Следвайки идеите на еволюционния подход при дефинирането на областта „информационни системи", Cohen (2009) въвежда понятието Informing Science (наука за информирането), интердисциплинарна наука, обединяваща различни дисциплини, които решават сходни проблеми, свързани с обмена на информация.

Науката за информирането е феномен, който изследва доставянето на информация в необходимата форма, формат и график, така че клиентите да имат възможност да я оползотворят максимално ефективно за нуждите си.

Понятието „система за информиране" надгражда понятието „информационна система", т.е. те включват не просто информационното обслужване във вид на подготвяне, обработка и предоставяне на дадена информация, но и начините за възприемане на тази информация, въздействието ѝ върху клиента, ефективността ѝ при формирането на знание. Науката за информирането, чийто предмет са системите за информиране, е обобщаваща рамка на процеса на информиране във всичките му аспекти, изучавани от различни области на науката, и в това си качество е метадисциплина. Гаковски дава следната дефиниция на информирането като процес, с който се занимава науката на информирането: „Информирането е науката и изкуството на практическия стремеж за повишаване на ефективността и ефикасността". В рамките на тази научна област задачата за количествено оценяване на ефекта от „информирането" се явява естествен научен проблем. Създаването на средства – модели, мерки, алгоритми, позволяващи количествено оценяване на ефекта от информирането, ще даде възможност за прогнозиране на резултата от процеса на информирането и следователно ще осигури рационално управление на дейността по информирането.

Тук трябва да отбележим, че в този случай практиката изпреварва теорията. На пазара от десетина година се предлагат програмни системи, чиято цел е по-ефективно и ефикасно информиране на клиентите. Такива са системите, обединени от наименованието „бизнес интелигентност" (data warehouses и data mining), системите за управление, ориентирано към клиентите (customer related management), системите за управление на съдържанието (content management systems) и др.

Модел на Коен

Моделът на система за информиране на Коен включва три основни компонента:

1. Метасреда за информиране (Informing Environment);

2. Система за доставяне на информацията (Delivery system);

3. Система за изпълнение на поставената задача (Task-completion system), като тези компоненти са поставени в контекста на науките за поведението (behavior sciences), специфичната проблематика за дадената предметна област и използваните технологии.

В определението „среда за информиране" Коен включва източника на информация и кодиращото устройство от класическия модел за комуникация по теорията на Шенън. За разлика от модела на Шенън средата за информиране се разглежда на три нива на абстракция: (1) използване на съществуваща система, (2) създаване на нова система за информиране, базирана на съществуващи принципи, и (3) създаване на нови принципи/нова рамка за изграждане на такива системи за информиране.

Коен илюстрира тези нива със следния пример от академичната сфера:

- Може да представим ниво (1) като преподаване на дисциплина от преподавател, който не я е разработил сам (в училищата обикновено учителите получават готов план за работа от Министерството на образованието и учебник, по който да преподават);
- Ниво (2) – като разработване на курс за обучение по дадена известна дисциплина, по която има достатъчно учебници, като се използва стандартна форма на обучение, например лекции, и преподавателят е свободен да комбинира съдържание и да определя последователността на изложението, за да постигне поставените цели;
- Ниво (3) – като създаване на нова дисциплина (формулиране на нови принципи, цели, парадигми) или разработване на нови подходи за преподаване на материала.

Целта на Средата е да осигури на клиента информация в определена форма, детайлност и последователност, така че той да има възможност да я оползотвори максимално ефективно за нуждите си.

Системата за доставяне на информацията е представена от информационните технологии, които използват системата за информиране. Това са модерните комуникации и компютри, чиято цел е

да подпомогнат средата в информационния процес. Тази система представлява междинният компонент от модела за комуникация (канала за комуникация), който отговаря за пренасянето и доставянето, но и за съхраняването на информацията с цел по-нататъшното ѝ изследване, разпознаване, обработка и представяне.

В комуникационния модел на Шенън липсва елементът „съхранение на информацията". За времето си просто той не е бил необходим, но с напредването на техниката и развитието на информационните технологии става възможно пренасянето на големи количества информация (вече се измерват не в битове, а в MB, GB, TB), което налага и тяхното съхранение.

Системата за изпълнение на поставената задача съответства на декодиращото устройство плюс получателя от модела на Шенън. Обикновено нуждата от информация възниква във връзка с решаването на някаква конкретна задача. Задачата, която си поставя клиентът, потребителят или мениджърът, вземащ решение, определя от каква информация се нуждае той. Това е принципно новото в този модел – поставя се акцент не толкова и не само върху механизма на доставка на информацията, но най-вече върху това за какво и как тя ще бъде използвана. Дефинирането на задачата опростява процеса на информиране и дава възможност рискът при информиране да бъде оценяван – ако този, който създава съобщението, знае за какво ще се използва изпращаната информация, той ще формулира съобщението в контекста на целта на потребителя.

Модел на Денчев

Стъпвайки върху създадената от самия него ТЕОРИЯ НА ИНФОРМАЦИОННАТА СРЕДА (**Денчев**, С. Информационна среда за трансфер на технологии. София: Захарий Стоянов, 2004), Стоян Денчев надгражда своите идеи, като в значителна степен се опира на класическия информационен модел на Шенън. Отделните структурни компоненти на Модела на Денчев може да се сведат до следните:

1. Информационна среда (обобщена или отделно взети „частни" информационни среди);

2. Информационен процес;

3. Съвкупност от комуникационни процеси;

4. Модел за оценка, интерпретиране и използване на информация.

Управление на процеса на информиране

От кибернетиката е известно, че без наличието на обратна връзка една система не може да бъде управлявана (виж например Weiner и Schoderbek, P., Schoderbek, C., Kefalas, A.). Само системи със затворен цикъл осигуряват информация, позволяваща вземане на решения за коригиране на поведението на системата, или с други думи – управление на системата. Друг важен аспект на управлението е необходимостта от количествено измерване на резултата от дейността на дадената система, което да позволи определяне на необходимостта от и размера на коригиращото действие. Тези две страни на управлението определят потребността от количествено измерване на рисковете в процес на информиране.

От особено значение е оценката на риска от мисинформиране, тъй като при такива събития не се наблюдават външни белези на отказ в системата, както при другите три категории рискови събития, при които не се осъществява информиране: отказ в комуникационния канал, невъзможност за разбиране на съобщението или отхвърляне на съобщението поради неприемане. При мисинформиране външно процесът изглежда успешен, страните в процеса не забелязват наличието на проблем, но резултатът може да бъде заблуждаване на получателя.

Дали значението на съобщението, вложено от източника, съвпада със значението, разбрано от получателя, и какъв е рискът от грешна интерпретация на съобщението, може да бъде оценено при наличието на обратна връзка – т.е. източникът да получи информация дали и доколко правилно получателят е разбрал и приел полученото съобщение. При това количественото оценяване на степента на заблуждаване е много важна, ключова необходимост.

Информационна асиметрия

За да се осъществи процес на информиране, трябва да е налице информационна асиметрия – едната страна (изпращачът) да знае повече по дадения въпрос, предмет на комуникацията, от другата страна (получателя). В противен случай комуникацията е безпредметна – получателят не получава нова информация и не генерира

ново знание.

Тази асиметрия често се изразява във формулиране на съобщението с използване на терминология, позната в дълбочина на изпращача, но чужда за получателя; в използване на приети в дадена предметна област концепции и постановки, но непознати за непрофесионалисти; в използване на професионален жаргон; в използване на полисемията на естествените езици и т.н.

Интерпретацията на съобщението е решаваща за това доколко то ще информира или мисинформира получателя. Успехът на този етап от комуникационния процес е силно повлиян от феномена информационна асиметрия.

При бизнес трансакции информационната асиметрия се наблюдава, когато едната страна в трансакцията има повече или подобра информация от другата стана. В икономиката такъв дисбаланс се използва за описание на определна пазарна ситуация, наричана „пазари с асиметрична информация", в която обикновено продавачът знае повече за продукта от купувача. Възможна е и обратната ситуация – например при застраховка на имущество купувачът на застраховката знае повече за скрити дефекти и проблеми от продавача.

Има няколко различни аспекта, в които се използва терминът „информационна асиметрия":

- Терминът „информационен дисбаланс" е употребен за първи път от Кенет Ароу (Arrow), който го въвежа като морален риск ("moral hazard"). По-късно Джордж Акерлоф (Akerlof) използва термина „асиметрична информация", показвайки, че в пазар с асиметрична информация средната стойност на стоката върви надолу дори за стоки с перфектно качество. Много изследвания, особено на финансовите пазари, продължават насоката на Акерлоф;
- Асиметричното влияние на позитивната и негативната информация на общественото доверие е познато като „принцип на информационната асиметрия" или „асиметрия на доверието". Тези изследвания са инициирани от Словак (Slovac) и са предмет на активна изследователска дейност;
- Значимостта на използването на информационната асиметрия за постигане на влияние при бизнес отношения е друга област, привличаща вниманието на много изследователи, която също има своите корени в работата на Акерлоф;

• Информационната асиметрия като източник на мисинформиране е областта, за която ролята на информационната асиметрия се приема за даденост. Този аспект на информационната асиметрия не е изучен до степента, която заслужава. Някои автори (виж Chang-Tseh Hseih, Fujun Lai, and Weihua Shi, 2006) разглеждат влиянието на информационната асиметрия върху успеха при бизнес трансакции, но те не отиват по-далеч от това да предложат стратегии за подобряване на процеса на информиране чрез възприемане на различни политики за обучение, като „информационно ориентиране“ и др.;

• По принцип целта на процеса на информиране е да предоставя информация от по-добре информираната страна на по-слабо информираната страна. Така информационната асиметрия е естествено необходима за процеса на информиране. От друга страна, информационната асиметрия е основна причина за възникване на мисинформиране.

С цел увеличаване на шанса за успех на процеса на информиране и намаляване на риска от погрешно разбиране (мисинформиране) е подходящо да се работи в две основни насоки:

• Намаляване на информационната асиметрия чрез обучение на източника и/или получателя на информация и приближаване на техните знания (например чрез използване на технологии като CRM);

• Предлагане на гаранции за покриване на риска от мисинформиране чрез споделяне на риска между двете страни.

ИНФОРМАЦИЯТА КАТО РЕСУРС: УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ

Информацията, в цялото разнообразие, в което се проявява, е ценен ресурс също като финансовите, материалните и човешките ресурси.

Най-общо казано, концепцията за информационните ресурси може да се изрази по следния начин: **ВСИЧКИ НАЛИЧНИ РЕСУРСИ НА ЕДНА СИСТЕМА И ТЯХНАТА ТРАНСФОРМАЦИЯ В ИЗПОЛЗВАЕМА ИНФОРМАЦИЯ**. Ако детайлизираме и осмислим професионално горното определение, бихме могли да го перифразираме в следната

ДЕФИНИЦИЯ: Информационни ресурси **(IR)** са всички физически и логически компоненти на системата за обработка на информация, като компютри, програми, данни, информация, операционни системи, комуникационни връзки, системни програмисти, програмни анализатори, оператори и мениджъри.

Глобализирането на икономиката води до разширяване на границите, в които една социална система работи. Нарастват броят и разнообразието както на директните конкуренти, така и на потенциалните клиенти и доставчици. Ако преди години за един търговец е било достатъчно да се разходи из чаршията, за да получи актуална пазарна информация, днес трябва да създаде организация, занимаваща се с непрекъснато сканиране на Средата. **Стойността на информацията нараства и тя (информацията) се превръща все повече в един от най-ценните ресурси.** От друга страна, с успешното или неуспешното решаване на всеки проблем организацията трупа опит – учи се, генерира свой уникален ресурс от знания, с помощта на който решава повече или по-малко ефективно и ефикасно възникващите проблеми.

Налице са два процеса: на непрекъснато нарастване на обема информация, който трябва да се обработи за решаване на даден проблем, и на повишаване на изискванията за обхватно, точно, цялостно и задълбочено анализиране на проблемната ситуация. От една страна, обемът информация, който трябва да се обработи, расте, а от друга, прецизността и сложността на обработката на информация също растат – по-голям обем информация, по-сложни методи за обработка. Решаването на тази дилема е в широкото използване на съвременни информационни – компютърни и комуникационни – технологии. Това от своя страна предполага преминаване от интуитивно към рационално вземане на решения. **От друга страна, мобилността на персонала създава условия натрупани във фирмата знания и опит да бъдат загубени заедно с напускането на хората – техни носители.** Това налага фирмите да създават система за регистриране и съхраняване на знанията, генерирани при решаването на проблеми.

Тоест информацията изисква целенасочено управление, което се означава с термина **„управление на информационни ресурси“ (IRM)** (или **„информационен мениджмънт“**). Под този термин се разбират следните дейности:

- **Управление на IT инфраструктурата**

– *Хардуер* – обхват и критерии:

  - **Технологии за съхраняване на данни** (*Storage Technology*): капацитет, способност за нарастване – *Scalability*);
  - **Обработващи технологии** (*Processing Technology*): скорост на обработка, достъпност, способност за представяне;
  - **Следене на насоките на технологично развитие**;

– *Софтуер:* Да купя или да направя?;

– *Организация:* централизирана или мрежова; изграждане като цял проект или чрез „острови“ и последваща интеграция; управление на данните (data management);

- **Управление на знанията** (knowledge management): преобразуване на интуитивно в експлицитно (записано) знание. Този процес следва следните фази (вж. фиг. 4):

Фиг. 4. *Процес на преобразуване на интуитивно в експлицитно знание*

– Създаване – решаване на проблем по нов начин;

– Хващане – разпознаване, че е открито ново знание;

– Рафиниране – процес на очистване на новото знание от конкретните параметри на ситуацията, която го е породила, и неговото обобщаване за по-широко приложение;

– Съхраняване – записване;

– Управление – включване на новото знание в инструментариума, използван за решаване на проблеми в организацията;

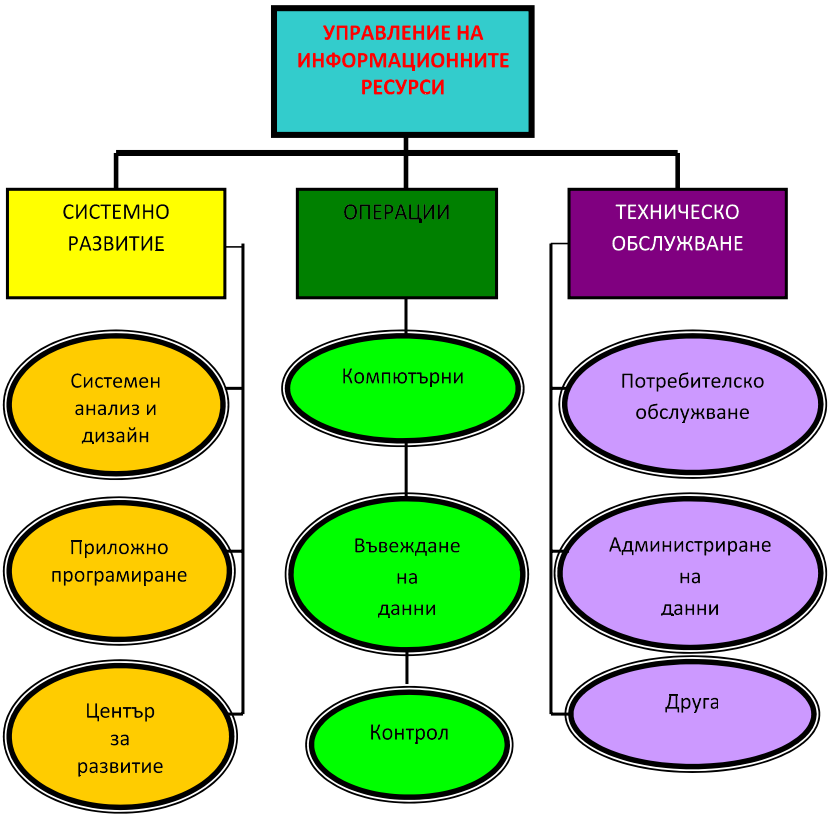
– Разпространяване – обучение;

– Абстракция – процес на преобразуване на знание за решаване на конкретен проблем в знание за решаване на клас проблеми;

• **Управление на развитието на персонала по отношение на информационните технологии;**

• **Управление на организацията и администрирането**.

Системите за управление на информационните ресурси (IRM) се състоят от организационните структури за управление на информационните ресурси (IR), асоциираните с тях правила за вземане на решения и итеративните комуникационни процеси между различните компоненти на IR.



Фиг. 5. *Функционално-организационна структура на информационното обслужване в бизнес организационна система*

IRM стана популярна терминология за подчертаване на основните промени в областта на управлението и на ролята на информацията в него. Това е нова концепция, която определя новото място и роля на организационната функция „информационно обслужване“. IRM дава основание да се твърди, че технологиите, свързани с информационното обслужване, промениха начините за правене на бизнес.

Във връзка с развитието на IRM много компании вече създават управленски позиции на високо ниво, които се наричат ГЛАВНИ ИНФОРМАЦИОННИ МЕНИДЖЪРИ (***Chief Information Officer – CIO***), с основна задача да наблюдават и управляват използването на IR в своите организационни структури.

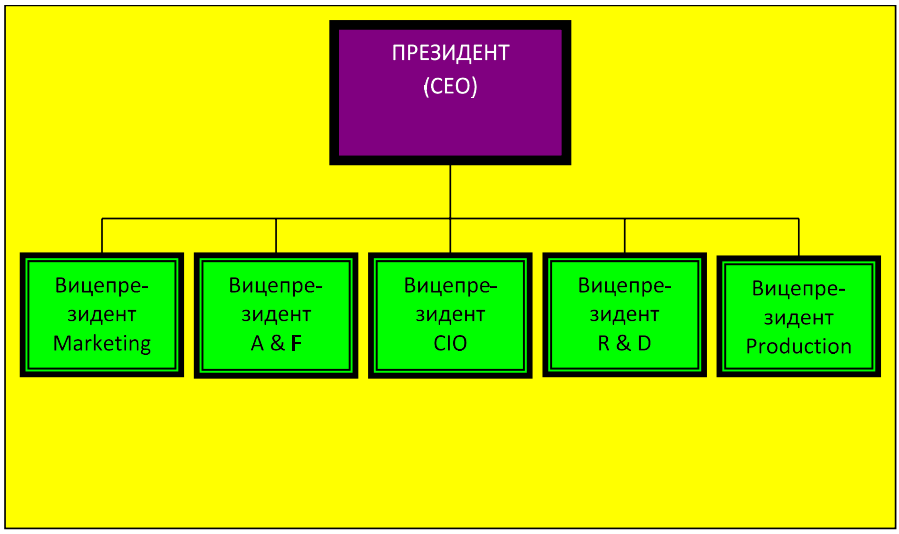
Компютърното обслужване, телекомуникациите, развитието, стратегическото и функционалното информационно обслужване, автоматизираните офис системи и всички други IT сервизи са отговорност на този нов вид управленец (executive). CIO не се занимава с ежедневното (операционно) информационно обслужване. Неговите активности са концентрирани в дългосрочното планиране и стратегиите.

CIO има функциите и задълженията на вицепрезидент на компанията и носи следните отговорности:

- Координира работата и дава директиви на мениджърите на базите данни, системните анализатори и проектанти, телекомуникациите и на всички офис системи;
- Подпомага стратегически останалия персонал, за да го приобщи към промените на техниката и технологиите, да му разкрива неговите информационни нужди;
- Следи за навлизането на най-новите технологии в системата;
- Организира информационната сигурност.

В този смисъл новите организационни диаграми, в стратегическото си ниво, имат структурата, показана на фиг. 6.

В много от управленските структури на съвременните компани функциите, задълженията и отговорностите на ГЛАВНИЯ ИЗПЪЛНИТЕЛЕН ДИРЕКТОР се припокриват с функциите, задълженията и отговорностите на ГЛАВНИЯ ИНФОРМАЦИОНЕН МЕНИДЖЪР, т.е. **CEO = CIO**.



Фиг. 6. *Съвременна управленска организационна диаграма*

СИГУРНОСТ

СЪЩНОСТ И СТРУКТУРА НА СИСТЕМАТА „СИГУРНОСТ“

ОБЩИ РАЗСЪЖДЕНИЯ ПО ТЕМАТА

Преди всичко, в самото начало на този раздел е необходимо да направим опит за определяне на категорията „сигурност“, а оттам – на системата „сигурност“.

Ето някои общи разсъждения по темата:

Сигурността е всеобща същност и начин на съществуване на материалния и духовния свят и на всички форми на тяхното проявление. Няма явление, отношение, процес или дейност, които да не съдържат в себе си, като свой същностен и градивен елемент, сигурността. Сигурността може да се отнесе към системата от категории като движение, пространство, време, енергия и информация. Сигурността е всеобщо и системно състояние на всичко съществуващо.

Сигурността отразява и изразява количествената и качествената определеност на всяка система, на нейното съществуване и развитие в съответствие със същността ѝ и собствената ѝ мяра. Сигурността събира в едно цяло разпръснатите зрънца на същността, дава простор на съществуването в строго определени рамки и чрез това запазва целостта и същността на системата. Сигурността е мяра в мярата на всяка системна структура. Тя се проявява като обективна и всеобща закономерност, чието подценяване или отричане води до хаос, разпадане и разрушаване на дадена система.

Сигурността се намира в непрестанно движение, промяна и развитие. Тя има свое начало, върхове и падения, свой край. И всичко това протича по силата на нейни специфични закономерности, произтичащи от особеностите на дадената обективна реалност. Системата „сигурност“ винаги е елемент на дадена природна и социална система, т.е. тя е система в системата и не може да съществува без нея. Тя е неин градивен елемент и същностна функция, което дава основания да се разглежда и като относително самостоятелна система. Основното е опасностите, заплахите и посе-

гателствата върху системата, идващи отвътре и отвън, да не надхвърлят същността и възможностите ѝ да се съхрани в определената ѝ мяра. Сигурността гарантира пълноценно, равномерно, стабилно и възходящо съществуване и развитие на системата, като своевременно открива и неутрализира всички възможни опасности, заплахи и посегателства върху нейната същност и съществуване.

Сигурността като система съдържа изискването да не е конфликтна с други, близки до нея системи. Обратното, да е в конкретни, съдържателни и ползотворни отношения и взаимодействия, които биха позволили тя да се съхрани, да се защити от различни опасности, да се опази, да оцелее, а чрез това да се гарантира сигурността на системата, чийто елемент е тя.

Сигурността като система, особено сигурността на социалните явления, отношения, процеси и дейности, може и следва да се разглежда като същностен и градивен елемент на социологическата структура на обществената система. От друга страна, при отсъствието на системата „сигурност" обществото може да се разпадне като система. Следователно може да се дискутира върху въпроса дали системата „сигурност" е елемент на социологическата структура на обществото, или не.

Във връзка с това теоретичните позиции, от които се тръгва при изследване на социологическата структура на обществената система, са следните:

1. Обществото е система, имаща специфична структура, функции, принципи и закони;

2. Обществото, като органична и обективно съществуваща система, се саморазвива, самоорганизира, саморегулира и чрез това се стреми да съхрани и да развие своята количествена и качествена същност, определеност, мяра и смисъл на съществуване;

3. Обществената система се ражда, съществува, функционира и се развива на основата на система от базисни, основни цели и интереси, потребности и дейности. Чрез тяхното постигане тя оцелява, съществува, обогатява се и се усъвършенства;

4. Социологическата структура е всеобхватна, обща, монолитна и е продукт, проявление на най-дълбоката и скрита природа на обществената система.

От тези позиции може да се формулират елементите на социологическата структура на обществото, в това число на информаци-

онното общество. Те са главната, интегрираща сила на социологическата структура на обществото, включително на гражданското и на информационното общество. В своята съвкупност те са системата от същност, цели, интереси, потребности и дейности на:

1. производството и възпроизводството на духовна култура и духовни блага и ценности;

2. човека като индивид и личност – раждане, отглеждане, възпитание, образование, квалификация и реализация;

3. комуникациите и комуникационните отношения, технологии, техника, връзки и движения на хора, вещи, идеи;

4. информацията, знанията, информационните отношения, информационните системи, технологии, техника и дейности;

5. управлението на социалните отношения – теория, технология, принципи, техника и процедури;

6. социалните отношения в тесния смисъл на думата – бит, нрави, обичаи, традиции, душевност на народ, нация, етнос, регион, семейство и други социални групи;

7. науката, научно-техническия прогрес, историята и съвременността на научното познание и тенденциите в неговото съществуване и развитие;

8. очовечаването, облагородяването и опазването на природната и околната среда;

9. глобалната, интегралната, всеобемащата, всепроникващата човешка цивилизация;

10. човека, човечеството, цивилизациите като единна система, която е елемент на Вселената, безкрая и вечността.

Възможни са и други подходи.

Ян Шчепански, полски социолог, приема, че обществото се състои от хора, вещи и отношения.

Т. Парсънс разглежда обществото като система от: индивиди, формална и неформална структура, ситуации и роли, физическо обкръжение. Човешкото действие, като саморегулираща се система, в отличие от физическото и биологическото действие има символичност, т.е. включва такива символически механизми, като език, ценности и др. На второ място, спецификата на тази система е в нормативността, т.е. съществува зависимост на индивидуалните действия от общоприетите ценности и норми, и накрая – в известна ирационалност и независимост от околната среда. Т. Пар-

сънс приема, че теорията за връзките и свързващите процеси има методологическо значение. Такива са комуникациите, равновесието и вземането на решение. Основен структурен принцип е функционалната диференциация. Социалната организация се определя като инструментален институт, като социална система, организирана за постигане на определени цели.

Алвин Тофлър привежда следните елементи на цивилизацията, а това в известна степен са елементи на обществената система: техносфера, биосфера, психосфера, сфера на силата, инфосфера, социосфера.

В друг, културологичен аспект Кенет Кларк приема, че цивилизацията е вяра, сила, енергия, жизненост, а ние може да прибавим – стремеж към промяна, сигурност и наличие на идеал.

Ако допуснем, че социологическата структура на информационното общество са онези негови елементи, посочени по-горе, може да се приеме, че това общество е отрицание на аграрната и промишлената цивилизация, на съответните обществени системи. То съдържа и ползва материалните и духовните достижения на аграрното и промишленото общество, но те не са неговата същност, смисъл и предназначение. Информационното общество се ражда, развива и функционира в сравнително кратко историческо време – от края на XX век вероятно до третата третина на XXI век. Като естествена основа за дефиниране и развитие на системата „сигурност", информационното общество:

1. поставя в основата на всичко съществуващо и имащо фундаментално значение за материалната и духовната същност и съществуване на обществената система информацията, познанието, знанието, образите, символите, данните, културата, ценностите и съответните технологии и техника;

2. дава неограничен простор на творческите, евристичните, съзидателните сили, възможности, качества на всеки индивид независимо от геополитическо, религиозно и социално положение;

3. представлява хуманитарна, демократична, аполитична обществена система;

4. извежда в символ, идеал интелекта на личността и човечеството;

5. създава условия личността да се себепознава и реализира като личност на света, без да губи националната си идентичност;

6. създава условия и предпоставки за съществуване и развитие на световни процеси и отношения, имащи глобална, общочовешка същност, смисъл и предназначение;

7. представлява висша степен в съществуването и развитието на гражданското общество;

8. предоставя възможности за зараждане и развитие в рамките на своето съществуване на нови и вероятно по-съвършени обществени системи и цивилизации.

СПЕЦИФИЧНИ ЕЛЕМЕНТИ НА СИСТЕМАТА „СИГУРНОСТ“

В пряка зависимост от съвременното информационно общество – основата на проявление на системата „сигурност“, нейните елементи са конкретизация на посочената по-горе същност на сигурността и фактически са нейно конкретно проявление, съществуване в определени области и състояния на материалното и духовното. От тези позиции като съставни елементи на сигурността може да се разглеждат:

1. Сигурността на всичко съществуващо, на обективните и реалните природни и социални дадености

В този смисъл сигурността е всеобщ природен и обществен закон, а системата „сигурност“ е същностен и градивен елемент на всяка възможна и съществуваща система. Сигурността в този случай е всеобща категория на всяко познание и има философско-социологическа същност, съдържание, форма и смисъл. Тя е системен елемент на всяка система независимо от нейното обективно или субективно съществуване и проявление, независимо от времето, пространството, енергията, информацията и движението. С еднаква сила и значимост тя се отнася за физическите, химическите, биологическите, социалните явления, отношения, процеси и техните проявления. Това означава, че системата „сигурност“ може и следва да се разбира като система с космическа същност, съществуване, функции, структура и измерения.

2. Сигурността на самата социологическа структура на обществото

Става дума за система на сигурност на обществото като цяло, като организъм и система, на неговото появяване, съществуване,

функциониране, развитие и евентуално отмиране. Тя се схваща като сигурност на обществото по отношение на природни явления, отношения и процеси, по отношение на света като цяло, нямащ начало и край, като общество и Вселена, общество и вечност, общество и други възможни общества, човешка цивилизация и други цивилизации, интелект и световен, вечен и всемогъщ интелект.

3. Сигурността на всеки от елементите на социологическата структура

Сигурността на един елемент пряко и косвено се отразява върху сигурността на останалите елементи на социологическата структура. Всяко отклонение от необходимата степен на сигурност, характеризираща нормалното съществуване и функциониране на даден елемент, закономерно води до нарушаване на сигурността и на другите елементи, увеличава опасностите, заплахите и посегателствата, дава простор на неравномерно и неравностойно съществуване на отделните елементи, което води до диспропорции, противоречия, конфликти, кризи и разруха.

4. Сигурността на субектите на гражданското общество: държава, социални обединения, организации и личността на гражданина

5. Сигурността на политическата, икономическата, социалната, правната и ценностната система, специфични за гражданското общество

6. Сигурността на всяко единично явление, отношение, процес и дейност, съществуващи в определен период от социално време, пространство, енергия и информация

7. Сигурността на самата система за сигурност

Тя съдържа: теоретична и технологична, информационна и управленска, стратегическа и тактическа, институционална, правна и професионална сигурност.

8. Системата от специализирани държавни и граждански органи и организации, имащи за цел и дейност охрана, опазване, защита на сигурността от всякакви опасности, заплахи и посегателства Върховенство на Закона, Морала и Професионализма във всичко и навсякъде, и за вечни времена – това е Законът, пронизващ цели, функции, структури, задачи и дейности на тези специализирани институции на системата „сигурност“.

9. Обединяващата функция на сигурността

Тя съединява в едно цяло останалите елементи на съществуващата система, като ги обединява, сплотява и оттук – премахва, ограничава, свежда до минимум наличието или зараждането на разностранни, по-големи и по-малки заплахи, опасности и посегателства.

10. Сигурност на националното, общонародното и общочовешкото, на човешката цивилизация и тяхното конкретно битие

Процесът на развитие от национална към гражданска държава, от промишлена към информационна цивилизация извежда на преден план общонародното и общочовешкото в материалното и културното битие на отделните народи и страни.

11. Гарантирането на свобода, демокрация, собственост, национален суверенитет и независимост, на социалногрупов, семеен и личен живот, бит, нрави, обичаи и традиции и недопускане на никакви посегателства върху тези светини за всеки гражданин

В този елемент по същество се съдържа сигурността на множество категории, понятия и състояния, имащи пряка връзка с категорията и системата „сигурност". Поради това може да се посочат и други понятия и категории, както и състояния, имащи връзка и взаимно влияние със сигурността, разбирана като категория и система.

12. Сигурността на международни, световни, икономически, политически, социални и ценностни явления, отношения, процеси и дейности

Световната социална сигурност е естествен и закономерен елемент на сигурността на гражданското общество.

13. Охраната, опазването и защитата на конкретната[7] социална обстановка, на нейната времева, пространствена, ергономична и информационна същност и определеност

14. Сигурност на възходящото развитие на личността, на професионализма, на нравствеността и хуманността

---

[7] Тук се има предвид *конкретност* в теоретичното и технологичното опознаване и въздействие върху строго определена област и в съответствие с мярата, която трябва да се следва, опазва, охранява, защитава и цялостно подкрепя и участва в процеса за нейната промяна и развитие.

Стабилност на правила за кариера, законност, морал и социална отговорност от всички и за всички.

15. Строго спазване на изискването, че всеки елемент е равнопоставен, равно значим и равносилен на останалите елементи и между тях няма и не може да има йерархия, подреденост по важност и значимост.

Вероятно е възможно да се посочат и други елементи на системата „сигурност", ако се ползват други изходни теоретични позиции и други разбирания за социологическото познание. По принцип всеки от елементите на системата „сигурност" е обект на изследване от отделна, частна обществена наука. В историята на научното познание и особено в съвременното научно познание за системата „сигурност" се оформя и развива специална научна система.

ИНФОРМАЦИОННО ПРОСТРАНСТВО И СИГУРНОСТ

Предмет на нашите изследвания тук са изучаването, анализът и управлението на информационна среда, съществуваща и развиваща се в специфичната предметна област „сигурност и в частност информационна сигурност".

Проблемите на сигурността и в частност на информационната сигурност и защита на класифицираната информация в компютърните системи за управление, търсещи своето решение в процеса на експлоатация на каквато и да е информационна среда, изискват да се спазват определени принципи още на етапа на нейното проектиране. Когато една информационна среда вече е „създадена" и се намира в експлоатация, е много трудно към нея да се добавя като кръпка цялостна система за информационна сигурност. От една страна, самата защита във всички случаи няма да е достатъчно ефикасна, а от друга, процесът на добавянето на такава система е неоправдано трудоемък. Друг е въпросът, когато за такава система се мисли още в процеса на проектирането на Средата. Съобразявайки се с принципите, които ще изброим по-долу, можем да сме уверени, че ще осигурим достатъчна степен на безопасност, секретност и защита на данните и информацията (информационна сигурност) в бъдещата експлоатация на информационната среда.

– **Първи принцип:** Удобство за потребителите. Връзката

между човека и оборудването на информационната среда, преминаваща през системата за информационна сигурност, трябва да бъде естествена и удобна за осъществяване и използване. В противен случай, при по-детайлно запознаване със системата, има значителна вероятност тази връзка да бъде „заобиколена“ по някакъв начин;

– **Втори принцип:** Минимум привилегии. На всеки потребител трябва да се дават само тези привилегии, от които действително се нуждае;

– **Трети принцип:** Простота и икономичност. Проектът на системата за информационна сигурност, а и самата система трябва да бъдат колкото е възможно по-прости и по-малки, като това, разбира се, не трябва да се отразява върху нейната ефективност;

– **Четвърти принцип:** Привличане на висококвалифицирани специалисти с цел откриване, отстраняване и контролиране на уязвимите от гледна точка на защитата на информацията места в проекта;

– **Пети принцип:** Проверка на пълномощията при всяко обръщение към всеки от защитените обекти;

– **Шести принцип:** Пълната информация, засягаща управляващите параметри на системата за безопасност, защита и секретност, трябва да е разделена по определени правила минимум между две оторизирани лица;

– **Седми принцип:** Ако се предвижда в информационните фондове на Средата да се съхранява съвършено секретна информация, последната не трябва в никакъв случай да се намира в бази данни с разделени ресурси.

Описаните основни принципи, които трябва задължително да се спазват при проектирането, е наложително да се съчетаят и с конкретни мерки и дейности при експлоатацията на въпросната информационна среда.

НАЦИОНАЛНА СИГУРНОСТ. СОЦИАЛНИ ИЗМЕРЕНИЯ

Националната сигурност е динамично променящо се състояние на обществото, при което са защитени основните права и свободи на гражданите, държавните граници, териториалната цялост и независимостта на държавата, когато не съществува пряка опасност от въо-

ръжено нападение, насилствена промяна на конституционния ред, политически диктат или икономическа принуда за държавата и гражданите и е гарантирано функционирането на държавните, местните и гражданските институции, в резултат на което обществото и нацията запазват и увеличават своето благосъстояние.

Гражданите, обществото и държавата имат задължения, записани в конституциите и законите на съответните страни, сами да са създатели и гаранти на своята сигурност. Едновременно с това те са взаимносвързани потребители на сигурност, като нарушаването на безопасността на който и да е от тях нарушава безопасността на останалите. Заедно те съставляват единната структура за сигурност на държавата.

Сигурността е гарантирана, когато държавата успешно реализира националните интереси, цели и приоритети и при необходимост е в състояние ефективно да ги защити от външна и вътрешна заплаха. Равнището на сигурност се определя от степените на защита и на ефективно реализиране на интересите на гражданите, обществото и държавата, които в съвкупност съставляват националните интереси.

Интересите на гражданите са в реалното гарантиране на конституционните права и свободи, личната безопасност, повишаването на качеството и равнището на живота, на социалното и здравното осигуряване.

Интересите на гражданското общество са в утвърждаването на демокрацията, гражданския контрол върху институциите и свободата на сдружаване, в правата на религиозните, етническите и малцинствените групи, в съхраняването на националните духовни и културни ценности и традиции.

Интересите на държавата изискват защита на конституцията, суверенитета и териториалната цялост на страната, постигане на политическа и финансова стабилност на икономическото и социалното развитие, строго спазване на правовия ред, равнопоставеност и взаимноизгодно международно сътрудничество.

Информационният фактор за гарантирането на националната сигурност действа чрез спазване на конституционните права и свободи на гражданите в областта на съхраняването и обмена на достоверна информация посредством развитието на модерни комуникации и медии. Опазването на националната сигурност изис-

ква да не се допуска използването на информацията за манипулиране на масовото съзнание. Приоритет е да се гарантира със специален закон защитата на държавния информационен ресурс от изтичането на важна за страната политическа, икономическа, научно-техническа и друга информация.

Удовлетворяването на основната човешка *потребност от сигурност* е довело до създаването на *система за национална сигурност*, която гарантира сигурността на българските граждани и осигурява защитата на интересите на гражданското общество, териториалната цялост и суверенитета на държавата. Тази система обхваща всички сфери на човешката дейност: политическа, икономическа, социална, духовна, външнополитическа, екологична, военна, вътрешнополитическа и информационна.

Системата за национална сигурност е голяма и сложна човеко-машинна система, в която съвременните технологии се използват за създаване, събиране, предаване, обработка, съхранение и потребление на информация. В тази система информационните и комуникационните технологии са средство, което усилва възможностите на човека в процесите на стратегическо ръководство, командване и управление.

Експлозивното развитие на науката и информационните технологии в края на XX век предизвика множество дълбоки промени в стратегическата среда. Тези промени засягат всички аспекти на обществения живот. Появиха се нови реалности, които най-общо се проявяват като рязко усложняване на международната обстановка, нарастване на обхвата и темпа на промените и поява на множество нови рискове и предизвикателства, пораждащи кризи и конфликти.

Нарастването на ролята на информацията в обществените процеси, глобалното разпространение на информационните инфраструктури, ръстът на информационния обмен и глобалната комуникационна интеграция на света свързват в единна мрежа градове, села, нации, човечеството като цяло. Тази пространствено-времева информационна интеграция създава множество нови възможности за възход и просперитет. Тя обхваща всички аспекти (политически, икономически, социални, културни, военни, екологични и информационни) на обществената активност в единно световно информационно пространство, което днес се превръща в системообразуващ фактор на развитието.

Дейността на обществените субекти в информационното пространство активно влияе върху състоянието на националната сигурност във всичките ѝ аспекти. Анализът на тенденциите в стратегическата среда ясно показва наличието на два глобални процеса, които са породени от експлозивното развитие на науката и технологиите, а именно:

• *трансформационен*, при който рутинните интелектуални функции на човека се прехвърлят върху новите оръдия и средства на труда, и

• *интеграционен*, при който всички подсистеми за управление на националната сигурност и стратегическо ръководство на отбраната и въоръжените сили се обединяват в единна обща метасистема (наричана още „система от системи“).

Тези два процеса фундаментално променят характера и структурата на обществените отношения и начините на упражняване на организирано насилие. В края на XX век информационният императив на развитието на човешката цивилизация внесе необратими промени в базовата аксиоматика на бъдещите конфликти, кризи и война, които са:

– машинно, а не човешко ориентирани;

– с характер и форми, произтичащи от технологии, а не от организации;

– с приоритет на възпиращите бойни действия, без човешки жертви и с минимални съпътстващи разрушения вместо въвличане в унищожителни сражения;

– поставени на индустриално-технологична, а не на командно-административна основа.

Тези промени предизвикаха радикални изменения в схващанията за националната сигурност. Те доведоха до излизане от употреба и унищожаване на три поколения военна техника в периода след Втората световна война и създадоха условия за формулиране на нови концепции и доктрини за водене на т.нар. „нетрадиционни войни“. *Днес националната сигурност на която и да е страна може да се гарантира само чрез изграждане на еволюционно развиващи се комплексни автоматизирани информационни системи за стратегическо управление, в които се анализират всички действащи фактори и се осигурява възможност за вземане на ефикасни решения. Разработката и използването на тези систе-*

ми изискват ясна информационна стратегия и ресурсно осигурен модел на техния жизнен цикъл, съгласувани с общата концепция за национална сигурност и развитие на страната.

Всяка национална информационна система за стратегическо управление обединява организационно всички системи, които участват в провеждането на политика и с които се гарантира сигурността в различните сфери на обществения живот (политическа, икономическа, социална, правна, културна, военна и т.н.). Тя се използва от всички държавни органи, които съгласно предопределените им от конституцията на страната функции осъществяват националната информационна политика. Те носят основната отговорност за неутрализацията на всички несанкционирани външни или вътрешни действия върху националното информационно пространство, извършени с цел отслабване или нарушаване на нормалното функциониране на държавата. Те трябва да предотвратят всяко пряко или непряко проникване в тази система, извършено с цел да се дезинформират органите, които вземат решения на различни равнища, или да се попречи да получат необходимата им информация. Тяхна е отговорността за провеждането на национално отговорна *политика за сигурност и отбрана в информационното пространство*.

Политиката за сигурност и отбрана в информационното пространство е система (комплекс) от знания и технологии за рационално използване на информационните инфраструктури и ресурси на държавата със стратегическа цел – защита на жизненоважните интереси на личността, обществото и държавата от заплахи в информационното пространство. Тези интереси най-общо включват:

- опазване на националния суверенитет в националното информационно пространство;
- създаване на благоприятни условия за материално, духовно и интелектуално процъфтяване на нацията;
- развитие на националния научен и образователен потенциал и разцвет на националната култура.

Оперативната цел на тази политика е да се подобри защитеността на държавните институции на страната, личността и обществото от заплахи в информационното пространство. По своята същност това е държавна дейност, произтичаща от възприетия

общополитически курс, осигуряващ най-благоприятни условия за развитие на обществото (държавата, личността) и гарантиращ националните интереси в информационното пространство чрез установяването на оптимално съотношение между структурните елементи на сигурността.

За да реализират успешно политиката за национална сигурност, органите на изпълнителната, законодателната и съдебната власт се нуждаят от информационни инфраструктури за съхранение, обработка и пренасяне на критична информация за планиране, ръководство, координация и контрол на текущите дейности. В тези инфраструктури има множество уязвими места, които може да бъдат атакувани и разрушени от специфични сили с голяма информационна мощ. Това се превръща в една от най-сериозните заплахи за националната сигурност на страната.

РЕГУЛИРАЩА ФУНКЦИЯ НА СЕКРЕТНОСТТА

Анализът на новите форми и способи за организирано насилие дава основание да се твърди, че структурно-функционалните промени и въвеждането на нови организации в системата за национална сигурност дават временен положителен ефект. Проблемът е, че протичащата трета технологична (информационна) революция непрекъснато променя вижданията за конкуренция, съперничество и противоборство в информационното пространство и анализаторите не успяват да завършат изследванията си преди появата на нови информационни средства и технологии. Не смогват цялостно да оценят новите свойства и характеристики на постоянно възникващите конфликти и кризи, тъй като те са функция на сложни взаимодействия, а проявяващите се ефекти са трудно наблюдаеми. Натрупаният до днес емпиричен материал е крайно недостатъчен, а моделирането на насилието в информационното пространство засега е само научна идея.[8] В същото време опитът от

[8] Относно моделирането на насилието в информационното пространство виж: **Kotenko**, I., A. **Ulanov**. Antagonistic agents in the Internet: Computer Network Warfare Simulation. Proceedings of Fusion '2006 Conference, Florence, Italy, 2006.

последните въоръжени конфликти показва, че *националната сигурност става все по-силно зависима от информационната и комуникационната свързаност на обществото*.

Всички жизненоважни обществени инфраструктури са силно свързани и нелинейно взаимодействат една с друга, което ги прави чувствителни към всякакви вътрешни и външни смущения. В националното информационно пространство протичат процеси с явно изразена нелинейна (хаотична) динамика. Нарушаването на функционирането на която и да е от националните автоматизирани информационни системи може да има неочакван косвен ефект върху цялата национална инфраструктура (енергетика, транспорт, финанси и т.н.). Този ефект не е пропорционален на смущенията и може да предизвика лавинообразно нарастващи катастрофални промени в цялата национална система, разпространявайки се по трудно предвидими вторични, третични и т.н. връзки. Като краен резултат се нарушава способността на държавата синергично да използва своята мощ за реагиране при бедствия, аварии, катастрофи, кризи, конфликти и война.

Засилването на връзката „информационни системи – инфраструктурна уязвимост“ налага по нов начин да се интерпретира сигурността на гражданите, обществото и държавата. Доколкото състоянията на мир, конфликт и криза са явно различими, то в обществото има цялостна представа за тях и определена подготовка за рационално поведение при преминаване от едно към друго. Основният проблем е свързан с мярата. Въпросът, който възниква, е: До каква степен намеренията, оперативните концепции, плановете и приготовленията трябва да бъдат публично оповестени?

Известно е, че публичността премахва действието на фактора изненада. И докато премахването на изненадата за отделните граждани и обществото като цяло е полезно и стабилизиращо, то за потенциалните конкуренти, съперници и противници е облекчаващо и опростяващо действията им обстоятелство. Независимо от степента на определеност и регулираност, особено при управление в извънредни ситуации, възникват следните въпроси: Каква е мярата за легално ограничаване на информираността на гражданите и обществото? Ако в мирно време субектите могат да упражняват правото си на информация до момента, в който засегнат правата на друг субект, то до каква степен могат да упражняват правата

си субектите при извънредно положение? *Тъй като субектите са носители на ясно определен обем права и задължения – кога, как и при какви условия този обем може да бъде променян? Как се регулира достъпът на гражданите до информация, така че да бъде както легален, така и легитимен?*

Секретността е инструментът, с който се регулират обществените отношения в сферата на достъпа до информация. Има множество инструменти за регулиране на обществените отношения, но основното различие между тях и секретността е, че докато с другите се определя какво могат да правят гражданите, то *секретността определя какво те не могат да знаят*.

Прилагането на секретността като инструмент се извършва при строго спазване на буквата и духа на законите и в съответствие с основните начала на конституцията на всяка отделно взета страна. Тъй като гражданските права и свободи заемат централно място в политическите системи на демократичните държави, конституционните норми налагат съществени ограничения на прилагането на този механизъм от субектите на властта. Съгласно конституцията на всяка отделно взета демократична държава всеки субект има право да търси, получава и разпространява информация. Осъществяването на това право се ограничава дотолкова, доколкото не може да бъде насочено срещу правата и доброто име на други граждани, както и срещу националната сигурност, обществения ред, народното здраве и морал. Всички граждани имат право да получат информация от държавен орган или учреждение по въпроси, които представляват за тях законен интерес. Това право може да бъде ограничено само дотолкова, доколкото тази информация не е защитена от закона тайна или не засяга други права. *На практика има две пречки пред разширяването на секретността:*

а) конкурентното действие на правото на информация на други субекти и

б) ограничаването на правото на държавата да въвежда секретност само в сферата на опазването на националната сигурност, обществения ред, здравето и морала на своите граждани.

Силата на възпиращото им действие се регулира в сферата на доверието на гражданите в ефективността на механизмите на политическата система и нейните субекти, което се захранва от гражданския контрол. Гражданският контрол е единствено

възможният механизъм за въвеждане на законосъобразна и целесъобразна мяра за секретност.

Гражданското общество изисква ефективни комуникации, съпричастност и кооперативност, които са немислими без *прозрачност* (т.е. гласност, откритост и отчетност). Прозрачността осигурява свободен достъп на гражданите до процеса на вземане на решения и участие във властта. Едновременно с това тя създава благоприятни условия за прогнозиране на организационното поведение и добиване на ясна представа за степента на удовлетвореност на желанията и реализация на очакванията. При всяко разминаване на очакваното с желаното крайно състояние се формират неудовлетвореност, разочарование, недоволство, отчужденост, затвореност и стремеж за промяна. Този стремеж е толкова по-силен, колкото по-голямо е разминаването между аз-идеално и аз-реално в отделната личност, което от своя страна води до появата на желание за друго поведение и друга политика. Когато разочарованието е масово, сработват естествените демократични механизми на гражданското общество и в изборния процес се раждат новите политически сили на промяната. Когато разочарованите индивиди са малцинство, няма перспектива за промяна и няма консенсус, се налага вотът на мнозинството. Малцинството трябва да търси удовлетворение в рамките на принудителната адаптация, което в повечето случаи е с цената на стратегически компромиси. В тези условия несъвършенствата на човешката същност раждат *идеята за конспирация като скрито нелоялно поведение*. Такова поведение може да доведе до появата на заплахи и рискове за сигурността на гражданите, обществото и държавата. *В редица изследвания върху секретността се доказва, че тя е единственият инструмент за ефективна защита от посегателствата върху националната сигурност.*

Секретността се институционализира от държавната администрация. Министерства и ведомства получават и обработват информация, като чрез засекретяване превръщат част от нея в тайни. Тайните са част от неосезаемите активи на властта. Поводът да се засекретява информация, е обективно съществуващата заплаха от загуба на информационно превъзходство и като следствие – загуба на наблюдаемост и управляемост на държавата. Разширяването на обхвата на секретността прави „непрозрачни“ всички критично важни части от националното информационно пространство. То се превръща в „черна

кутия“ за анализаторите на потенциалните конкуренти, съперници и противници. Борбата за информационно превъзходство над тях стимулира увеличаването на тайните. Тъй като в „непрозрачно“ информационно пространство се вземат лоши решения или изобщо не се стига до решения, постигането на необходимата осведоменост е жизненоважно за успеха на всяко социално управление.

Осведомеността се постига с разузнаване, а завоюването на информационно превъзходство изисква още контраразузнаване. Характерна особеност на тези професии е, че се упражняват скрито от обществото. По своята същност те са скрита форма на осъществяване на политическа практика, целите и задачите на която са да се завоюва информационно превъзходство. Три нови модела на поведение влизат в живота на социалните организации:

- *конспирация*,
- *лоялност* и
- *секретност*.

Всяка от тях се институционализира и създава обслужващи административни органи. Заплахите за националната сигурност се зараждат и развиват в условията на заговорничество и конспирация. С помощта на специално законодателство се създават условия за изкореняване на нелоялността и подривната дейност чрез въвеждането на режими на секретност. Така се гарантира националната сигурност, но се ограничават гражданските свободи.

Формирането на моделите на лоялността и заговора ражда като последствие необходимостта от скриване на критично важните за реализацията на организационната мисия сведения от нейните нелоялни членове. Това от своя страна налага да се дефинират и институционализират концепциите за секретността и тайната. Тук трябва да се поясни, че зачитането на гражданските свободи се превръща в проблем на оценката на лоялността. Свободата поражда многообразие, което трудно се управлява без въвеждането на ограничаващи йерархии. Законодателството на либералните демокрации дава възможност за широка изява на „свободната воля“ на всеки гражданин, което затруднява обективното оценяване на дадено поведение като лоялно или нелоялно. При тази съществена неопределеност става трудно да се оценят заплахите и рисковете за сигурността. Ангажираните с нейното гарантиране са принудени да отчитат това обстоятелство чрез повишаване на секретността,

т.е. чрез увеличаване на *сведенията, фактите и обстоятелствата, определени като класифицирана информация*.

Основно задължение на държавните институции е гарантирането на сигурността на гражданите. Държавните субекти са тези, които формулират *списъка на категориите информация, подлежащи на класификация като* ***държавна тайна***. Властта отговаря на заплахите с разпоредби, осигуряващи лоялността на хората и гарантиращи опазването на държавната тайна. Съответно се приемат разпоредби срещу нелоялно поведение от страна на гражданите. Те вкарват организационното поведение в рамките на възприетата политика и стратегията за реализацията ѝ. Най-съществено е, че тайните се генерират от и в държавните институции, които могат да използват това предимство така, както намерят за добре. Това създава възможности за формиране на неравнопоставеност между гражданите и държавата, размерите на която не трябва да превишават реалните нужди на гарантирането на националната сигурност, обществения ред, народното здраве и морал.

Идеята за лоялност предполага по необходимост и идеята за секретност. Нелоялните служители биха издали тайни, а лоялните – не. В обстановка на недоверие и подозрителност нарастват опасенията, което увеличава обхвата на секретността. Все повече неща се засекретяват. Това стимулира развитието на системата от нормативни актове, регулиращи защитата на класифицираната информация, което от своя страна циклично реверсивно увеличава неравнопоставеността между гражданите и държавата, която непрекъснато се увеличава. Носещите отговорностите за сигурността, реда, здравето и морала на обществото непрекъснато увеличават служебните тайни, ограничават кръга на професионално осведомените за своите знания и намерения. Те провеждат „секретни“ заседания, с които се премахва прозрачността и се затруднява гражданският контрол. Понятието „служебна тайна“ е специфично бюрократично изобретение на професионалната общност на публичната администрация. Във взаимодействие с парламента бюрокрацията се стреми към засилване на наблюдаемостта и управляемостта на държавата, което се усилва от инстинкта за запазване на властта и често води до формално (принудително) съдействие на парламентарните разследвания. Така описаната обратна връзка се усилва от превръщането на секретността в норма, при което култу-

рата на бюрокрацията поражда култура на секретност.

Секретността обаче може да се превърне в заплаха за демократичното общество, тъй като напълно осведомената общественост е основата на самоуправлението. Хората, които са избрани и назначени на длъжности в изпълнителната власт, не могат да бъдат помъдри от целия народ. Това е истина, която не се споделя охотно сред управляващите. *Тайните са актив, който, съчетан с други ресурси, се превръща в базови компетенции. Тези компетенции са извор на конкурентоспособност, която трудно се споделя.*

Връзката „сигурност – секретност" е явна и очевидна. Потребността от опазване на държавните тайни не се нуждае от коментар. Връзката „секретност – конкурентоспособност" е косвена, сложна и невинаги забележима. Оценка на този циклично-реверсивен цикъл може да се направи както от гледна точка на обществения морал, така и от позициите на социалното управление. Етичните аспекти на секретността са тема на други изследвания. Обект на разглеждане подолу са информационните аспекти на връзката „сигурност – секретност", което е актуално и значимо за хората, вземащи решения. За тях е най-добре всички информационни източници, даващи необходимите за вземането на разумни решения знания, да са открити. Откритостта формира климат на доверие, в който хората не се притесняват от разногласия, неясноти и колебания. Всички разбират как да се оползотворят богатството и разнообразието на явната и общодостъпна информация. В тези условия тайното събиране на сведения и трупането на тайни от ръководителите не са добра линия на поведение. Те могат да дадат по-добра осведоменост, но ограничават активността, креативността, творчеството и като цяло – възможностите за професионална изява на членовете на организациите. Стратегическото мислене и анализът са много по-добри инструменти от секретността за постигане на сигурност и информационно превъзходство. Трябва да сме наясно, че 95% от всичко, което е необходимо да се знае, може да се извлече чрез обработка на информацията от явни източници на информация, открити и публично достъпни през интернет. Останалите 5% може лесно да се изведат с аналитични инструменти. Секретността започва там, където започват проблемите на националната сигурност, обществения ред, здраве и морал. Там се установява *регулаторна рамка*, създаваща баланс между секретност и прозрачност в сферата на държавното управление.

НОВА СТРАТЕГИЯ ЗА СИГУРНОСТ. КИБЕРСИГУРНОСТ

ИНФОРМАЦИОННА СИГУРНОСТ И ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Автоматизирани информационни системи и мрежи за управление при бедствия, аварии и катастрофи

Информационна сигурност

Информацията е един от основните ресурси, който се използва във всеки аспект от живота на човека и вследствие на това се нуждае от защита. Слабите места в защитата на информацията могат да доведат до нанасяне на различни и многобройни вреди. Създадена е голяма нормативна и теоретична база, както и математически модели, които описват словесно повечето понятия, свързани с информационната безопасност. Историята и практиката на различните кибератаки, различни по цели, обхват и интензивност, доказват колко е важна темата за информационната сигурност (3).

Една от най-общите дефиниции за *информационна сигурност* е: защитата на информацията и системите от неоторизиран достъп, разкриване, промяна, унищожаване или „пробиване".

Трите основни цели на информационната сигурност са:

• Поверителността/конфиденциалността се отнася до защита на информацията от неоторизиран достъп или разкриване.

Осигуряването на поверителност гарантира, че онези, които са оправомощени за достъп до информация, са в състояние да направят това, а тези, които не са упълномощени, са възпрепятствани да го направят. Терминът „поверителност" („конфиденциалност") се отнася до защита на важна информация от разкриване от неупълномощени потребители.

Степента, до която трябва да бъде поддържана поверителността, зависи от типа информация, за която се прави опит за защита.

• Интегритетът се отнася до защита на информацията от не-

разрешена промяна или унищожаване. Осигуряването на интегритет гарантира, че информацията и информационните системи са точни, пълни и неподправени. Целостността на данните означава гарантираност, че данните не са променяни от неупълномощени потребители.

• Наличността/достъпността се отнася до защита на информацията и информационните системи от неоторизирано прекъсване на достъпа до тях. Осигуряването на наличност е осигуряване на своевременен и надежден достъп до и използване на информацията и информационните системи. Терминът „достъпност“ не е ограничен до достъпност на информация, той включва достъпност на системите и останалите ресурси, необходими за достъп до информацията.

Информационната сигурност може да се приеме и като „сигурност на данните“. Повечето съвременни данни се намират в електронен вариант на сървъри, настолни компютри, лаптопи или някъде в интернет – но преди десетилетие, преди цялата поверителна информация да се прехвърли онлайн, е присъствала в хартиен вариант в шкафа в кабинета. И все още доста от поверителната информация се намира там. Информационната сигурност се занимава с осигуряването на сигурността на данните под всякаква форма и е по-широка от киберсигурността. Някой може да бъде експерт по сигурността на информацията, без да е експерт по киберсигурността.

Управлението на информационната сигурност сега е нормален и обикновен елемент в публичното пространство. Стряскащи думи като хакерство и киберсигурност са популярна тема за разговор между ежедневните потребители на технологии, а информационната сигурност е в челните редици на притесненията на хората.

Запознавайки се с дефиницията за информационна сигурност, отнесена в контекста на организацията като звено, можем да я използваме за основни познания, които да ни послужат за определяне на културата на киберсигурност. А именно информационната сигурност е състояние, отнасящо се към информационен ресурс, в което се осигуряват, поддържат и гарантират:

– непрекъснатост на зададените процеси;
– минимизация на рисковете към ресурса;
– недопускане на отказ на достъпа до информационните ре-

сурси (сигнали, данни, знания, култура) и инфраструктури;

– недопускане на несанкционирано ползване, манипулиране или разрушаване на тези ресурси;

– недопускане на отслабване в каквато и да е степен или премахване на възможностите за създаване, събиране, разпространение, обработка, съхранение и ползване на информация без разрешение;

– недопускане на несанкционирано ползване, манипулиране или разрушаване на инфраструктурата ѝ.

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 равнище. Политиката за информационна сигурност е множество от правила и практики, които определят как организацията управлява, защитава и разпределя информацията. Политиката най-често обхваща:

- достъпните ресурси и услуги;
- контрола върху достъпа;
- правила за идентификация и автентикация;
- използвани методи за защита на данните от различни атаки;
- обучение и подготовка на потребителите.

Основните цели на политиката за информационна сигурност са:

- да подготвя специалисти, които да се стремят към осигуряване на техника и утвърждаване на нормативи за гарантиране на защита срещу злоупотребата с информация;
- да утвърждава отговорностите и отчетността на ръководители и служители за информационните ресурси;
- да утвърждава изискванията за поверителност на информацията и начините за контрол и достъп на различните видове персонал;
- да предотвратява нарушаването на управленските функции на ръководния състав в случай на загуба или злоупотреба с информация.

Според някои стандарти информационната сигурност се свежда до запазването на поверителен характер, конфиденциалност, цялостност, достъпност и наличност на информацията; може да бъдат добавени и други свойства, като автентичност, достоверност, отговорност, отчетност, невъзможност за отказване от авторство (non-repudiation) и надеждност (ISO/IEC 17799-2005).

Като критични фактори за успешното прилагане на информационната сигурност литературата и опитът на специалисти класира следните по-важни условия като добра основа за изграждане на ефективна сигурност на информационните ресурси:

- разбиране на изискванията за информационна сигурност, на необходимостта от определяне и управление на риска;
- политика за информационна сигурност;

Информационната сигурност цели въвеждането на контрол на достъпа до информационните ресурси, запазването на целостта на информацията и нейния конфиденциален характер.

Постигането на добра информационна сигурност неминуемо се предшества от процесите на идентификация, анализ, оценка, приемане и управление на риска.

АВТОМАТИЗИРАНИ ИНФОРМАЦИОННИ СИСТЕМИ. МРЕЖИ

Всяка автоматизирана информационна система (АИС) е съвкупност от технически и програмни средства, методи, процедури и персонал, организирани за осъществяването на функции по създаването, обработването, съхраняването, ползването и обмена на информация в границите на дадената системна организационна структура. Тя може да бъде изградена както в мрежа, така и на базата на една или повече отделни работни станции, несвързани в мрежа.

Мрежи. Компютърни мрежи. Видове

Мрежата е съвкупност от технически и програмни средства, методи и ако е необходимо, персонал и процедури, организирани за осъществяване на обмен на данни (информация) между две или повече АИС или в рамките на една АИС.

Компютърните мрежи се разделят на две главни категории:

- равноправни и
- базирани на сървър.

При равноправната мрежа всички компютри са равнопоставени. Обикновено всеки компютър работи и като сървър, и като клиент. Мрежата няма конкретен администратор, а потребителите сами определят какви ресурси да поделят в мрежата. Системата за

сигурност се състои в задаване на парола за всеки ресурс, като например поделена директория или устройство. В равноправна мрежа всеки потребител настройва сам своята система за сигурност, поради което централизираният контрол е труден. Това оказва голямо влияние върху сигурността на мрежата, защото някои потребители може изобщо да не въведат никаква защита. Затова, ако сигурността е важен фактор, се изгражда мрежа, базирана на сървър.

При мрежите, базирани на сървър, има компютър, работещ само като сървър, без да се използва като работна станция. С нарастването на размера и трафика на мрежите се появява нуждата от повече от един сървър. Разпределянето на задачите между няколко сървъра позволява мрежата да работи по-ефективно. Сървърите на големите мрежи трябва да бъдат специализирани, за да задоволяват нуждите на потребителите.

Основното предимство на мрежите със сървър е, че използването на данните може да се администрира и контролира централно. Сигурността може да се управлява от един администратор, който установява правилата за защита и ги прилага към всеки потребител от мрежата. Освен това, тъй като важните данни са централизирани на един или няколко сървъра, редовното им архивиране се осъществява и контролира по-лесно. Данните на всеки сървър може да се дублират така, че дори нещо да се случи с основната област за съхранение, където се намират оригиналните данни, те да може да бъдат възстановени от резервното копие.

Комуникационната система е съвкупност от взаимносвързани комуникационни средства, криптографски средства и среда за разпространение на сигнала, предоставящи *комуникационен ресурс* на АИС или мрежата.

Използваните технически и програмни средства за създаването на АИС или мрежа, както и потребителската и системната информация в тях са ресурсите на тази АИС или мрежа. Мрежовите ресурси може да се разделят на физически и информационни. Физическите ресурси са оперативната памет, процесорът, входно-изходните устройства и др. Информационните ресурси са програмните продукти и данните, които се съхраняват и обработват от физическите устройства. Ресурсите на мрежите се използват за представянето на пакет от системни и потребителски услуги, като:

- обмен на данни от различен тип;

- обмен на електронна поща в мрежата;
- търсене на услуги и ресурси по мрежата;
- комуникации между клиенти на мрежата;
- администриране, контрол, управление, защита и развитие на мрежата.

Архитектура на системите и мрежите

Архитектура на отворените системи. Налагането в глобалното информационно пространство на унифицирана архитектура на мрежите като отворени системи води след себе си дейност по стандартизация във всички аспекти на обработката на данните. Много съществен е проблемът за физическото предаване на информацията по различните видове комуникационни канали, кодирането на информация с контрол на грешките при предаване, маршрутизацията на информационните потоци, логическото поддържане на диалога между процеси, прехвърлянето на данни между системи с различно представяне, включително при криптографиране и декриптографиране, и пр. Тези проблеми се решават на програмно ниво. Международната организация по стандартите ISO дефинира модел на отворените системи със седем слоя в мрежовата архитектура:

1. Физически – определя начина на предаване на информацията в преносната среда;

2. Канален – определя достъпа до управлението на канала за предаване, както и коригирането на грешките при предаване;

3. Мрежов – засяга въпросите на адресация в мрежите;

4. Транспортен – определя начините за транспортиране на информационните обекти в мрежата и доставянето им между потребителите в мрежата;

5. Сеансов – определя способите за логическа връзка между отделните процеси в различни възли на мрежата;

6. Представителен – определя въпросите за преобразуване на данните между системите, включително въпросите за криптографирането;

7. Приложен – определя основните въпроси за предоставяне на приложни услуги на крайния потребител на базата на долните слоеве от мрежовата архитектура.

Процесите в едноименните слоеве на два отдалечени възела

комуникират по определени протоколи, а съседните протоколи в един възел си обменят данни по определени интерфейси. Физическата среда за предаване на данните може да се разглежда като нулев слой, а потребителите – като осми слой на архитектурата.

Съвременни мрежови архитектури. Когато говорим за високи технологии, трябва да имаме предвид, че те много динамично се развиват и търсят начини за постигане на оптимални решения на проблемите. Най-честият начин на реализация на съвременните мрежови услуги е да бъдат изградени по схемата „клиент – сървър". Поддържането на услугите в мрежата става чрез два процеса, в двата възела на мрежата, които комуникират помежду си. Процесът, който протича във възела, предоставящ услугата, се нарича сървър, а процесът, който протича във възела, употребяващ услугата – клиент. Клиентът търси подходящи сървъри, превежда заявката на крайния потребител в достъпен за сървър вид и я изпраща. **Процесът – сървър** се инициира от постъпилата заявка, изпълнява я и връща резултата на **процеса – клиент**. Процесът – клиент представя резултатите от изпълнението на заявката в подходящ за крайния потребител вид.

За потребителите най-важно е да познават методите за адресация и търсене на абонатите на мрежата и достъпните за тях услуги, предлагани от мрежата. Ползвайки част от тези услуги, потребителят може да получи информация за всички ресурси и услуги и започвайки от елементарното, да достигне до овладяване на голямо разнообразие от тях.

Основното предимство на клиентската част при модела „клиент – сървър" е наличието на широк избор от приложения, средства за разработка, опитни програмисти и потребители с достатъчни компютърни познания. Приложенията, които изискват голяма компютърна мощ, използват ресурсите на клиентската машина, а автономността на клиента улеснява администрирането на сървъра. Освен това разпределените в сървъра приложения намаляват част от натовареността на клиента и може да бъдат по-добре защитени.

Напоследък моделът „клиент – сървър" се модифицира в концепцията Intranet. Тя позволява да се изгради корпоративен интернет, свързан чрез firewall (защитна стена) към мрежата. Предимствата на този модел са, че: приложенията може да бъдат достигани от всеки мрежови компютър; намаляват се времето и инвестициите

за обучение на потребителите; хардуерът и операционната система на клиентската станция остаряват значително по-бавно, тъй като се поддържа само софтуер за търсене на документи.

Приложенията от сървъра са достъпни веднага за всеки оторизиран потребител в интернет/интранет. Тъй като цялата поддръжка и осъвременяване се извършват на сървъра, не е необходимо да се инсталира, поддържа каквато и да е част от клиентски софтуер. Такава организация може да поддържа огромен брой потребители, като дава възможност за добавяне на графичен потребителски интерфейс към старите терминали и предимно текстови приложения.

Ключово място във всички информационни системи имат създаването и поддържането на пълен и точен модел на информацията и данните, които представляват интерес за потребителя. Опростено погледнато, данните са факти, които са организирани по определен начин и са предназначени за използване при решаването на дадена задача. Информацията е сведение, намаляващо неопределеността. Количеството ѝ се измерва в битове, а качеството – с ценността. Тя се оценява субективно, в зависимост от ситуацията и потребителя.

Бази данни

В съвременното технологично развитие използването на АИС и мрежи е невъзможно без създаването на бази данни (БД). Базата данни е съвкупност от данни, организирани за общо ползване в рамките на различни изчислителни процеси. За нейното създаване, поддържане и използване се използва система за управление на бази данни (СУБД) с езикови и програмни средства. Основни функции на СУБД са:

- транслация на схемата на БД;
- създаване и верификация на БД;
- изпълнение на запитвания към БД;
- актуализация на данните в БД;
- копиране и възстановяване на БД;
- защита на БД чрез управление на достъпа и криптографиране.

Основни елементи при създаването и работата с бази данни са обектите и субектите на АИС или мрежи. Обектът на АИС или мрежа е пасивен елемент, чието качество е да съдържа или да приема информация. Субектът на АИС или мрежа е активен елемент,

представляващ лице, процес или устройство, притежаващо качеството да осъществява обмен на информация между обектите или да изменя състоянието на системата или мрежата. Създаването, обработването и съхраняването на класифицирана информация, както и използването на бази данни с класифициран характер в АИС или мрежи не се различава като организация и методи на работа от всички останали мрежи. Единствената разлика е необходимостта от сериозно гарантиране на сигурността им и защитата от заплахи от нерегламентиран достъп.

Защита на информацията в автоматизираните информационни системи за управление при бедствия, аварии и катастрофи

По-долу се представя системата от възгледи и основни принципи, които са в основата на решаването на проблема със защитата на информацията в автоматизираните информационни системи (АИС) и компютърните системи и мрежи (КСМ) от нерегламентиран достъп. Този проблем е част от проблема на информационната сигурност и засяга планировчиците, проектантите, създателите, собствениците и потребителите на АИС и КСМ, които ги използват за създаване, обработка, съхранение и пренасяне на информация и които имат нужда от защита на информацията.

Изложената система от възгледи и принципи е целесъобразно формирана методологична основа от нормативни и технически документи, която може да се използва като концептуална основа за разработката на изисквания за защита и сертификация на компютърните системи, мрежи и автоматизираните информационни системи от нерегламентиран достъп.

Защитата на класифицираната информация в компютърните системи за управление при бедствия, аварии и катастрофи засяга всяка автоматизирана система за обработка на информация и управление, всеки компютър и всички компютърни мрежи, използвани и/или администрирани от дадена организационна единица, в които се създава, обработва, съхранява и пренася информация. По-нататък ще наричаме тези системи, компютри и мрежи АИС или мрежи, така както това е възприето в регулиращите тази материя нормативни документи.

Тук се приема, че има две самостоятелни сфери на защитата на

информацията от нерегламентиран достъп:

- на автоматизираните информационни системи;
- на компютърните системи и мрежи.

Разликата се състои в обстоятелството, че компютърните системи и мрежи се произвеждат и доставят като градивни елементи, от които впоследствие се изграждат предметно и функционално специализирани автоматизирани информационни системи. На практика, без приложения, компютърните мрежи и системи не съдържат потребителска информация и не са автоматизирани информационни системи.

Освен потребителска информация, при създаването на всяка автоматизирана информационна система се формират нейните специфични характеристики, технология на обработка на информацията, права на потребителите и модели на заплахите. Защитата на информацията от нерегламентиран достъп в автоматизираните информационни системи и защитата на автоматизираните информационни системи от несанкциониран достъп са еквивалентни и равнозначни понятия. При компютърните системи и мрежи защитата на информацията се свежда до защита на процесите на създаване, обработка, съхранение и пренасяне на информация. В този смисъл защитеността им от нерегламентиран достъп е потенциално свойство (капацитет) да се затрудни такъв достъп до информацията в автоматизираните информационни системи, в които се използват компютърни системи и мрежи.

Нерегламентиран достъп до класифицирана информация

При анализа на общия проблем на информационната сигурност се очертават основните направления, в които преднамерената или непреднамерената човешка дейност може да доведат до нерегламентиран достъп. Това са неизправностите и отказите на техническите средства, наличието на грешки в програмното осигуряване, излъчването на паразитни електромагнитни или акустични излъчвания, природните бедствия, авариите и катастрофите. Всички те могат да доведат до нерегламентиран достъп във вид на нежелателно изтичане, модификация или унищожаване на информация.

Нерегламентиран достъп до класифицирана информация са разгласяването, злоупотребата, промяната, увреждането, пре-

доставянето, унищожаването на класифицирана информация, както и всякакви други действия, водещи до нарушаване на защитата ѝ или до загубване на такава информация. За нерегламентиран достъп се смята и всеки пропуск да се класифицира информация с поставяне на съответен гриф за сигурност или неправилното му определяне, както и всяко действие или бездействие, довело до узнаване от лице, което няма съответното разрешение или потвърждение за това.

Заплахи за автоматизираните информационни системи или мрежи

Заплахите са събития или действия, поставящи в опасност даден обект. Заплаха за АИС или мрежа е всяка възможност за случаен или целенасочен нерегламентиран достъп до създаваната, обработваната, съхраняваната и пренасяната информация. Заплахите се появяват при наличие на уязвимост.

Уязвимост на АИС или мрежа е слабост в системата от мерки за сигурност или в контрола за тяхното изпълнение, които могат да доведат до компрометиране или да улеснят компрометирането на сигурността. Уязвимостта може да бъде пропуск или да се дължи на недостатъчно ефективен надзор, недобра комплектуваност и устойчивост на работата или неефективна физическа защита. Уязвимостта може да бъде от техническо, програмно, технологично или процедурно естество. Наличието на уязвимост създава възможности за реализация на събития или действия, поставящи в опасност организацията (т.е. заплахи), в резултат на което може да настъпят *вреди*.

Вреда в областта на АИС или мрежа е увреждане на интересите на техните потребители (или на интересите, които те защитават), вредните последици от което не може да бъдат елиминирани или смекчени само с последващи мерки. В зависимост от значимостта на интересите и сериозността на причинените вредни последици вредите са: непоправими, или изключително големи; трудно поправими, или големи; ограничени.

Непоправими, или изключително големи, вреди са тези, при които е настъпило (или би могло да настъпи) цялостно или частично разрушаване на АИС или мрежата или е извършено непоправимо посегателство върху интересите на свързаните с тях потребители.

Трудно поправими, или големи, вреди са тези, при които е оказано (или би могло да се окаже) значително негативно въздействие върху АИС или мрежата (или върху интересите на свързани с тях потребители), което не може да се компенсира без настъпването на вредни последици, или вредните последици може да бъдат смекчени само със значителни последващи мерки.

Ограничени вреди са тези, при които е оказано (или би могло да се окаже) краткотрайно негативно въздействие върху АИС или мрежата (или върху интересите на свързани с тях потребители), което може да се компенсира без настъпване на вредни последици, или вредните последици може да бъдат смекчени с незначителни последващи мерки.

Заплаха за АИС или мрежа могат да бъдат всички техни обекти (пасивни елементи, съдържащи или приемащи информация) и субекти (активни елементи – лице, процес или устройство, обменящи информация между обектите или внасящи изменения в състоянието на АИС или мрежата). Тези заплахи може да се класифицират в четири йерархично подредени нива, всяко от които включва стоящото под него, както следва:

I ниво: Обхваща възможностите за водене на диалога в АИС или мрежа и изпълнението на ограничено множество задачи (програми), реализиращи предвидени функции по обработката на информация.

II ниво: Обхваща възможностите за създаване и изпълнение на собствени програми с нови функции по обработката на информация.

III ниво: Обхваща възможностите за управление на функционирането на АИС или мрежа, с които се въздейства върху базовото и програмно осигуряване и върху състава и конфигурацията на оборудването.

IV ниво: Обхваща възможностите на лицата, заети с проектирането, разработката, внедряването, експлоатацията и ремонта на АИС или мрежа, включително възможностите за включване на собствени програмни или технически средства с нови функции за обработка на информацията.

Познаването на възможните заплахи, както и на уязвимите места на АИС или мрежа, които тези заплахи експлоатират, дава възможност да се подберат най-ефективите средства за защита.

Трябва да се отбележи, че самото понятие „заплаха“ в различни ситуации често се тълкува по различен начин. Например за подчертано „открити“ организации може да не съществува понятието „заплаха за конфиденциалността“ – цялата информация е общодостъпна. В много случаи обаче нерегламентираният достъп е сериозна заплаха.

Много чести и доста опасни от гледна точка на загубите са грешките поради некомпетентност и невнимание на потребителите, операторите, системните администратори и други лица, обслужващи информационните системи. Понякога такива грешки са като заплахи (неправилно въведени данни, грешка в програмата, която би могла да доведе до срив в системата), а понякога създават слаби места, от които би могло да се възползват определени сили. Пожарите и наводненията може да се сметнат за нищожни, ако се сравнят с неграмотността и безотговорността. Най-радикалният начин за борба с неволните грешки са максималната автоматизация и строгият контрол на правилността на извършените действия.

Съществени по размери на загубите са преднамерените действия на лица и организации с цел нерегламентиран достъп. В резултат на подобни незаконни действия ежедневно се нанасят значителни щети, като в повечето от разследваните случаи виновниците са щатни сътрудници на организациите, отлично запознати с режима на работа и мерките за защита. Това илюстрира обстоятелството, че вътрешните заплахи са не по-малко опасни от външните. Много опасни са действията на т.нар. „обидени служители“ – настоящи и бивши, които са ръководени от желание да нанесат вреда на организацията, като например:

- да повредят оборудването;
- да внедрят „логическа бомба“, която да разруши програми или данни;
- да въведат неверни данни;
- да променят данни и т.н.

Необходимо е да се следи при напускане на служители, запознати с порядките в организацията, правата им за достъп до информационните ресурси да бъдат анулирани или прекратени своевременно.

Заплахите, идващи от физическата среда, в която е разположена и работи една информационна система, се отличават с голямо разнообразие. На първо място трябва да бъдат посочени нарушенията на инфраструктурата:

- аварии в електрозахранването;
- временна липса на връзка;
- пробив във водоснабдяването и пр.

Природните бедствия (пожари, наводнения, земетресения, урагани, ниско качество и сривове в електрозахранването) по статистически данни допринасят за 13% от загубите в информационните системи.

Опитите за нерегламентиран достъп до конфиденциална информация са една от заплахите, но опасността е голяма тогава, когато това се върши от лица, свързани с чужди разузнавателни структури или терористични организации. Почти всеки интернет сървър по няколко пъти на ден става обект на опити за проникване, но рядко тези опити се оказват успешни. Обикновено те се правят от лица, които имат големи познания в областта на компютърните и програмните технологии (т.нар. *хакери*) и за които е предизвикателство проникването в добре защитени системи. Като цяло загубите, предизвикани от дейността на хакерите, в сравнение с тези от други заплахи не са големи.

По аналогичен начин стои и въпросът за заплахата от компютърни вируси. **Вирусите по същество представляват програми, притежаващи способността да се размножават в операционната среда на компютъра, да създават копия със способност за по-нататъшно размножаване.** Този процес може да доведе до затрудняване на трафика на данни в мрежата и до пълното ѝ блокиране. Съвременната техническа литература, посветена на компютърните вируси, изобилства с екзотични наименования, като „червеи“, „логически бомби“, „троянски коне“ и пр., като същевременно се правят опити да бъдат класифицирани многобройните вируси, разпространени в мрежата. Някои видове вируси могат да нанесат големи щети, унищожавайки информацията. Независимо от това, ако са открити навреме и ако е създадена една съвременна защита в системата или мрежата, те може да бъдат предотвратени. Съблюдаването на елементарни правила на компютърна „хигиена“ до голяма степен понижава риска от загуби.

Заплаха към АИС или мрежа е възможността за случаен или целенасочен нерегламентиран достъп до класифицирана информация, създавана, обработвана, съхранявана и пренасяна в АИС или мрежа. Тези заплахи може да бъдат:

- Нарушаване на установения ред и организация за ползване на информационни услуги, включително нерегламентиран достъп, събиране и използване на класифицирана информация от бази данни и знания;
- Използване на несертифицирани или забранени методи за създаване, събиране, обработка и потребяване на информацията;
- Разработване и разпространяване на продукти, нарушаващи нормалното функциониране на националните информационни системи, включително на средствата и системите за защита на информацията;
- Неправомерни въздействия върху системите за защита на информацията, включително използване на несертифицирани наши и чужди информационни средства и технологии за защита на информацията или компрометиране на ключовете и средствата за криптографска защита;
- Унищожаване, повреждане, радиоелектронно подавяне или разрушаване на средства и системи за създаване, събиране, обработка и потребяване на информация;
- Внедряване на електронни устройства за прехващане на информация в технически средства за обработване, съхраняване и предаване на информация по свързочни канали, както и в служебни помещения на органите на държавната власт, местното самоуправление, учрежденията, организациите и предприятията независимо от формата им на собственост;
- Допускане на изтичането на информация по технически причини;
- Унищожаване, повреждане, разрушаване или грабеж на средства за обработка или носители на информация;
- Нарушаване на законовите ограничения за разпространяване на информацията.

Източниците на заплахи биват външни и вътрешни. Външни източници може да бъдат:

- Враждебни действия на чуждестранни организации, групи от хора и отделни личности от политически, икономически и ра-

зузнавателни структури, които целят нерегламентиран достъп до класифицирана информация;

• Дейност на международни терористични организации, целяща проникване в информационните системи на държавни, военни и други структури, които имат отношение към сигурността на държавата;

• Дейност на космически, въздушни, морски, наземни и други технически разузнавателни средства на чужди държави, събиращи класифицирана информация.

Към вътрешните източници на заплахи може да се отнесат:

• Враждебни действия на отделни личности в самите организации, които работят с класифицирана информация;

• Пропуски в нормативната база, регламентираща тези отношения, както и неефективно прилагане на закона;

• Некомпетентност на служителите;

• Недобра координация между държавните органи за прилагането на Закона за класифицираната информация, както и структурни реформи, извършвани в организационните единици (например приватизация);

• Изостаналост по отношение на техническите и информационните ресурси от водещите тенденции в света;

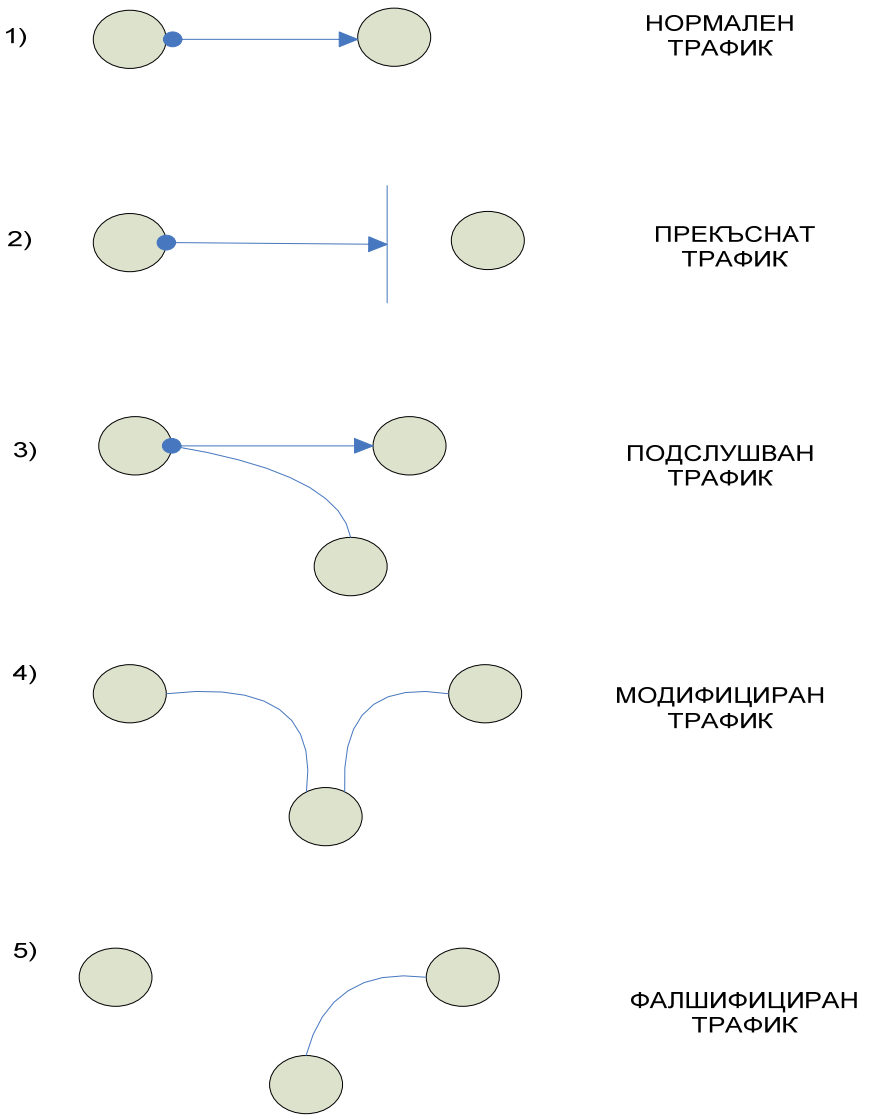
• Използване на несертифицирани в съответствие с изискванията на закона мрежи и системи за работа с класифицираната информация;

• Недостатъчно финансиране на мероприятията по организацията на защита на класифицираната информация;

• Предизвикани от човешка дейност технически аварии, както и природни бедствия в организациите и пр.

Модел на заплахите за сигурността на автоматизираните информационни системи или мрежи

Известни са пет различни варианта на модела на заплахата, като са дефинирани четири категории атаки срещу автоматизираните информационни системи или мрежи (фиг. 7).



Фиг. 7. *Варианти на модела на заплахите в автоматизираните информационни системи или мрежи*

Различните обекти се разглеждат абстрактно, т.е. като самостоятелни работни станции, обменящи данни или комуникационни средства, управляващи поток от данни и обменящи служебна информация за пътищата за предаване на данните. Вариантите на модела са, както следва:

1. Трафикът протича нормално, без да има наличие на външна намеса или нерегламентирано подслушване;

2. Налице е прекъсване на нормалния трафик – едно от ценните (жизнените) качества на системата е разрушено или е невъзможно използването му. Прекъсването може да бъде по най-различни причини, например проникване в глобалната среда за сигурност, довело до прекратяване на нормалния трафик;

3. Регистрирано е подслушване на трафика или пресрещане (прехващане) – едно неоторизирано действие дава достъп до системата. Подслушването може да се осъществява отдалечено, като чрез подходяща апаратура се прехваща излъчваният сигнал, моделира се и се привежда в удобен четящ вид. Подслушване може да се реализира и при непосредствен достъп до комуникационната система, било то до кабели, компютри, комутатори, сървъри или маршрутизатори;

4. Има модифициране на трафика. При този вариант, след като прехване трафика, третото „лице“ го подправя и го изпраща на крайния му потребител;

5. Изфабрикуван (подменен) е оригиналният трафик. В този случай има симулиране на трафик, като се подменят данните от изпращача и по този начин крайният потребител губи реална представа за истинския автор на получения от него трафик.

Прехващането е пасивна атака, когато няма намеса в комуникационните канали. Единственото нещо, което се осъществява, е постоянно наблюдение на преминаващата информация, докато прекъсването, модифицирането и изфабрикуването са активни атаки, тъй като там се регистрира намеса на трети „лица“.

Типове атаки

Най-често използваните атаки срещу автоматизираните информационни системи или мрежи може да се обобщят в седем категории:

- Кражба на пароли – методи за получаване на чужди потребителски пароли;
- Социален инженеринг – придобиване на информация, до която нямате достъп;
- Грешки и задни врати (bugs and backdoors) – получаване (използване) на преимущества посредством използване на системни грешки;

• Възможности за автентикация – използване на дефектите (противоречивост и непълнота) на механизмите за автентикация;

• Грешки (провали) в някои протоколи – протоколи с грешки в проектирането и реализацията;

• Изтичане на информация – използване на системи, като системата за подписване (finger) или системата за именуване (DNS), за информация, необходима на администратора или за функционирането на мрежата, но която може да се използва и за мрежови атаки;

• Отказ от обслужване – опити за лишаване на потребителите от услугите на тяхната компютърна система.

Категоризация в зависимост от резултатите

Тази категоризация е съставена в зависимост от постигнатите от атаката резултати:

• Разрушаване – при него има логическо разрушаване на комуникационните канали (например VPN) и физическо разрушаване, като прекъсване на кабели;

• Изтичане – пробив или уязвимост в системата, довели до изтичане на информация;

• Отказ (блокиране) – вследствие на атаката се е получило блокиране на системата, което за известно време (в зависимост от предприетите политики може да се намали или увеличи времето за реакция) прави системата неизползваема.

Емпиричен списък

Емпиричната класификация на заплахите позволява да се дефинират осем категории. Основното преимущество на тази класификация е, че съществуват атаки, които логически не могат да попаднат в точно една от трите изброени по-горе групи и които се обхващат от следната класификация:

• Външна кражба на информация;

• Външна злоупотреба с (на) ресурсите;

• Представяне (преструване; записване и използване на мрежовия трафик);

• Вредителски програми (инсталиране на злонамерени програми);

• Повторение на автентикацията или авторизацията (разбиване на пароли);
• Злоупотреба с авторизацията (фалшифициране на записи);
• Злоупотреба с бездействие (лошо администриране);
• Индиректна злоупотреба (като се използват други системи за създаване на зловредни програми).

Анализ на атаките

При наличие на атака трябва обстойно да се анализират уязвимите точки, довели до нея. За пълния анализ на атаките е целесъобразно всяка атака да се разглежда (класифицира) в следната последователност:
• хакери (атакуващи);
• средства, използвани при атаката;
• достъп до автоматизираната информационна структура;
• постигнати резултати при атаката;
• цели на атаката.

Класификацията на атакуващите компютърните мрежи и системи е във вида: хакери – правят го заради предизвикателството и статуса на получили достъп; шпиони; терористи; корпоративни нарушители; професионални престъпници; вандали.

Атакуващи и тяхната първична мотивация

Достъп

Основното свързващо звено между атакуващите и техните цели е неоторизираният достъп или неоторизираното използване на ресурсите в автоматизираната информационна структура или мрежа. Неоторизираният достъп или използване са свързани също с процесите или с файловете и данните, предавани по мрежата чрез процесите.

Неоторизираният достъп и използване са един от начините (пътищата) за атака. Не трябва да се пренебрегва и фактът, че са възможни и атаки при злоупотреба с правата за достъп. Не помалко от 80% от проникванията в системите са от напълно оторизирани потребители, които са злоупотребили с правата си за достъп. Това е потенциално и един от най-големите проблеми при защитата на автоматизираните информационни системи или мрежи.

Уязвимост

Най-често атакуващите използват предимствата на компютърната и мрежовата уязвимост. Уязвимостта може да се използва, както следва:

• Чрез софтуерните (хардуерните) грешки (bug). Типичен пример са Unix системите, които са в основата на Internet (Intranet) и които имат много проблеми в sendmail програмата, която често се използва за получаване на неоторизиран достъп до Host компютъра;

• Като се използват грешките, възникнали при проектирането на системите. Internet sendmail е типичен пример за това;

• Грешките, възникнали при конфигурирането на системите – те включват такива проблеми за сигурността, като системни правомощия с добре известни пароли, разрешение по подразбиране за използване на нови файлове; и др.

Резултати

Между придобиването на достъп и целите на атакуващите са резултатите от атаката. В тази точка от последователността на една атака атакуващият получава достъп до желаните процеси, файлове и данни. В този момент той е свободен да използва този достъп за чувствителните файлове, да забрани услуги, да получи информация или да използва услуги.

Средства

Средствата за атака може да се разделят в следните категории:

• Потребителски команди – въвеждани от командната линия или посредством потребителски графичен интерфейс;

• Скриптове или програми – стартирани от атакуващия и използващи уязвимостта на системите;

• Анонимни агенти – инсталират се програми или фрагменти от тях, които впоследствие работят независимо от потребителя и използват уязвимостта на системата;

• Средства за разработване – софтуерни пакети, съдържащи скриптове, програми или анонимни агенти;

• Разпределени средства – средствата за атака се разпределят върху различни компютри;

• Извличане на данни – когато се подслушва електромагнитното излъчване от компютърните системи или мрежи чрез устройства, външни за мрежите.

Оценка, анализ и управление на риска в компютърните системи или мрежи

Риск е вероятността за настъпване в определен период от време на събитие, оказващо негативно въздействие върху АИС или мрежа. Той е възможност (измерена количествено) за реализация на заплаха, т.е. възможност да се използва уязвимостта на АИС или мрежа, за да се компрометира в някаква степен тяхната сигурност.

Най-често рискът се свързва с неопределеността и неяснотата относно получаването на резултати от определени действия. С него се отчита възможността да се спечели или загуби при дадена съвкупност от събития. Измерването на степента на несигурност при извършването на човешките дейности е възприето да се нарича *оценка на риска*. В този смисъл основната цел на рационалното управление на информационната сигурност е да се минимизира рискът при зададено желано равнище на разходите за това. От това следва, че ефективната политика за информационна сигурност изисква предварително да се оценява и управлява рисковият компонент при вземането на управленски решения.[9]

Оценката на риска е процес на определяне на приоритетите в управлението на риска чрез оценяване и сравняване на нивото на риска с предварително определени стандарти, целево (приемливо) ниво на риска или други критерии.

Управлението на риска е процес на идентификация и контрол на опасностите с цел съхраняване и оптимално използване на ресурсите. В съвременната практика на управлението този процес се декомпозира на пет фази: идентификация на заплахите; оценка на заплахите и изчисляване на риска; създаване на система за управление на риска и вземане на решения; осигуряване на управлението на риска; контрол и оценка.

Анализът на риска за сигурността на АИС или мрежа е процес, при който се установяват заплахите и уязвимите места на АИС или мрежата, вероятността за осъществяване на заплахите при конкретните ресурси и работна среда и се оценяват последствията от тяхното реализиране. С него се целят:

---

[9] **Матеев**, М. Анализ и оценка на риска при избор на инвестиционни решения. София: Стопанство, 2000, с. 8.

1. Определяне на необходимите мерки за сигурност;

2. Ефективно комбиниране на видовете мерки за сигурност;

3. Правилна оценка на остатъчния риск.

Анализът на риска се извършва периодично с оглед отчитането на:

1. новопоявили се уязвимости и/или заплахи към АИС или мрежата;

2. промени в ресурсите на АИС или мрежата и/или в нивото на класификацията за сигурност на информацията.

За анализ на риска и определяне на адекватни мерки за противодействие се сформира екип от специалисти по физическа, персонална, документална, компютърна, комуникационна и криптографска сигурност и по защита от електромагнитни излъчвания. В този екип може да се привличат и представители на проектантите. За сложни АИС или мрежи при възможност се използват автоматизирани средства за оценка на риска.

Възможните резултати от анализа на всеки конкретен риск са:

1. Елиминиране на риска – целта е цялостно елиминиране на реална или потенциална уязвимост на АИС или мрежата чрез пълно прилагане на мерки за сигурност;

2. Предотвратяване на загубата на физически и информационни ресурси. Целта е прилагане на мерки за предотвратяване на загубите, доколкото това е възможно, като се отчита, че някои рискове не може да бъдат елиминирани поради технологични или други причини;

3. Ограничаване на загубата на физически и информационни ресурси – целта е прилагане на мерки за сигурност, ограничаващи загубите до приемливо ниво;

4. Приемане на риска от загуба на физически и информационни ресурси – когато загубата не е голяма, вероятността за загуба е малка или цената на необходимите мерки за предотвратяване на загубите е много голяма.

Резултатите от анализа на риска се оформят във вид на *Описание на специфичните заплахи, уязвимостите на АИС или мрежата, режима за сигурност при експлоатация на системата, изискванията към физическата и техническата среда*.

За условия на експлоатация на АИС или мрежа, които не са свързани с конкретна глобална среда за сигурност (например мо-

билни, полеви и други условия), при анализа на риска се оценяват и рисковете, свързани със средата, в която АИС или мрежата ще бъдат ползвани.

Основни способи за нерегламентиран достъп

Основните способи за нерегламентиран достъп до АИС или мрежи са:

- Пряк контакт с обектите на достъп;
- Създаване и използване на програмни и технически средства за контакт с обектите на достъп чрез заобикаляне на средствата за защита;
- Модификация на средствата за защита така, че да се осъществи контакт с обектите на достъп;
- Внедряване на механизми, които нарушават структурата и функциите на техническите или програмните средства така, че да се осъществи контакт с обектите на достъп.

Основни принципи на защитата от нерегламентиран достъп

Защитата на АИС или мрежа от нерегламентиран достъп се осигурява от действащите закони, стандарти и методически документи (нормативно), програмно-технически средства (технологично) и поддържащи административни мероприятия (организационно). Тази защита се осигурява през всички етапи на обработката на информацията и във всички режими на работа, в това число при провеждането на ремонтни и възстановителни работи.

Програмно-техническите средства за защита трябва да не влошават основните функционални характеристики на автоматизираните информационни системи (надежност, бързодействие, гъвкавост и структурно-функционална адаптивност).

Неразделна част от защитата е оценката на ефективността ѝ, която се получава с методика, отчитаща цялата съвкупност от технически характеристики на оценявания обект, включително техническите решения и практическата реализация на средствата за защита. Тази методика се прилага чрез въвеждането на периодичен или целеви контрол, извършван от контролиращите органи.

Основни насоки на работата по защита от нерегламентиран достъп

Защитата от нерегламентиран достъп се осигурява чрез:

- Система за разграничаване на субектите от обектите на достъп;
- Средства за осигуряване на разделен достъп.

Основните функции на системата за разграничаване на достъпа са:

- Въвеждане и реализация на правила за разграничаване на достъпа на субектите и техните процеси от данните;
- Реализация на правила за разграничаване на достъпа на субектите и техните процеси от устройствата за генериране на копия на информационни носители;
- Изолация на програмите и процесите, изпълнявани в интерес на един субект, от останалите;
- Управление на потоците данни с цел предотвратяване на записи на данни на носители, несъответстващи на маркировката;
- Реализация на правила за контрол на обмен на данни между субектите на АИС или мрежа.

Основните функции на средствата за осигуряване на разделен достъп са:

- Идентификация и разпознаване на субектите и поддържане на връзката между тях и изпълняваните за тях процеси;
- Регистрация на действията на субектите и техните процеси;
- Предоставяне на възможности за изключване и включване на нови субекти и обекти на достъпа, като и за промяна на правата им;
- Реагиране на опити за нерегламентиран достъп, например сигнализация, блокиране, възстановяване след такъв опит;
- Тестване;
- Прочистване на оперативната памет и работните области на магнитните носители след приключване на работата на потребителите;
- Отчет на изходните печатни, графични и други форми на изваждане на информацията;
- Контрол върху цялостната програмна и информационна част на средствата за осигуряване на разделен достъп.

Всички ресурси за осигуряване на разделен достъп се смятат за

обекти на достъп. Способите за тяхната реализация зависят от конкретните особености на АИС или мрежата.

Възможни са следните начини за реализиране на защитата от нерегламентиран достъп:

- Изграждане на разпределена система за разграничаване на достъпа с вградено в програмно-техническия комплекс ядро за защита;
- Вграждане на система за разграничаване на достъпа в операционната система, СУБД или приложните програми;
- Вграждане на система за разграничаване на достъпа в средствата за управление на мрежата или на нивото на приложенията;
- Използване на криптографски преобразования или методи за пряк контрол на достъпа;
- Програмна и/или техническа реализация на система за разграничаване на достъпа.

Основни характеристики на техническите средства за защита от нерегламентиран достъп

Основните характеристики на техническите средства за защита са:

- Степен, пълнота и качество на обхвата на правилата за разграничаване на достъпа, реализирани в системата;
- Състав и качество на осигуряващите системата за разграничаване на достъпа и осигуряващите средства;
- Гаранции за правилността на функционирането на системата за разграничаване на достъпа и осигуряващите средства.

Пълнотата и качеството на обхвата на правилата за разграничаване на достъпа се оценяват по наличието на ясни и непротиворечиви, заложени в система за разграничаване на достъпа правила за достъп на субектите и мерките за тяхната надеждна идентификация. Отчитат се също възможносите за контрол върху разнообразните процедури за достъп.

При оценяването на качеството на осигуряващите системата за разграничаване на достъпа средства се отчитат средствата за идентификация на субектите, редът за тяхното използване, пълнотата, отчетът на действията и способите за поддържане и привързване на субектите към процесите. Гаранциите за правилност на работата се оценяват по:

• начините на проектиране и реализация на системата за разграничаване на достъпа и средствата, които я осигуряват (формална и неформална верификация);

• състава и качеството на средствата, препятстващи заобикалянето на системата за разграничаване на достъпа (поддържане на цялостност и възстановяване след откази, аварии и опити за нерегламентиран достъп, контрол на диспечирането и възможности за тестване, контрол и диагностика по време на експлоатацията).

Оценяваната АИС или мрежа трябва да са щателно документирани. В състава на документацията се включват Ръководство за потребителя на защитните механизми и Ръководство за управление на средствата за защита.

Оценката на АИС или мрежа с висока степен на защита се извършва на основата на цялата проектна документация (идеен, технически и работен проект), а също така на описанията на процедурите за тестване и техните резултати.

Характеристики на класификацията на АИС или мрежа

Тази класификация е необходима за по-детайлна и диференцирана разработка на изискванията за защита от нерегламентиран достъп, с отчитане на специфичните особености на тези системи и мрежи. В основата на класификацията са следните характеристики на обектите и субектите на защитата и способите на взаимодействие между тях:

• Информационни – определящи ценността на информацията, нейния обем и ниво на класификация, възможните последствия от неправилната работа на системата или мрежата поради загуба или разрушаване на информация;

• Организационни – определящи правата на потребителите;

• Технологични – определящи условията за обработка на информацията (например начините на обработка – автономен, многопрограмен и т.н.), времето на пренос (трансфер, запомняне и т.н.), вида система или мрежа (автономна, мрежа, стационарна, подвижна и т.н.).

Организация на работата по защитата на АИС или мрежа от нерегламентиран достъп

Организацията на работата по защитата на АИС или мрежа от нерегламентиран достъп е част от общата организация на работата по информационната сигурност. Организационните мероприятия се реализират от потребителя на системата, а отговорността за тяхното внедряване се възлага на проектанта и създателя на системата или мрежата. Проверката на качеството на реализацията се извършва чрез комплексна оценка на сигурността, наричана „акредитиране".

Организационното осигуряване на защитата се основава на *Задължителни общи изисквания* в областта на физическата, персоналната, документалната, комуникационната, криптографската и компютърната сигурност и защитата от паразитни електромагнитни излъчвания. Те се определят от служителя по сигурността на АИС или мрежата на базата на общата политика за сигурност на организационната единица. На тази база се изготвят и специфичните изисквания за сигурност на АИС или мрежата, процедурите за сигурност и изработените на тяхната основа експлоатационни документи по сигурността.

Държавните органи по акредитиране на сигурността (ОАС) на АИС или мрежа са различни в различните държави. В съответствие с приетата процедура за акредитиране се извършва комплексна оценка на АИС или мрежата преди въвеждането им в експлоатация. При положителна комплексна оценка ОАС издава сертификат за сигурност на АИС или мрежата.

РЕГУЛИРАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В САЩ, ЕВРОПЕЙСКИТЕ СТРАНИ И РУСКАТА ФЕДЕРАЦИЯ

Проблемът за сигурността на информацията води до създаването на система от критерии и методологии за оценка на защитеността на информационните системи в редица напреднали в технологично отношение държави. Необходимостта от унификация и стандартизация в тази област налага познаването на съвременните постижения в тази сфера. По-долу е направен кратък преглед на

състоянието на регулирането в сферата на информационната сигурност във водещите държави.

Критерии за оценка на надеждни компютърни системи в САЩ („Оранжевата книга“ на Министерството на отбраната на САЩ)

Този труд, наречен така заради цвета на обложката си, е публикуван в САЩ през 1983 г. В него се говори за надеждните, а не за сигурните системи, като думата „надеждност“ се тълкува като нещо, на което можеш да се довериш. Очевидно е, че абсолютно сигурни системи не съществуват, че това е абстракция. Всяка система може да бъде превзета, ако се разполага с достатъчно големи материални и времеви ресурси. Има смисъл да се оценява само степента на доверие, която е разумно да се оказва на една или друга система.

Определението, което „Оранжевата книга“ дава за надеждна система, е: **„система, използваща достатъчно технически и програмни средства, така че да се осигури едновременната обработка на информацията с различни степени на секретност от група ползватели, без да се нарушат правата на достъп“**. Степента на доверие, или надеждност, на системата се оценява по следните два критерия:

- Политика за сигурност – това е набор от закони, правила и норми на поведение, които определят как организациите да обработват, защитават и пренасят информацията. Колкото по-надеждна трябва да бъде системата, толкова по-строга и всеобхватна трябва да бъде и политиката за сигурност. Политиката за сигурност е активният компонент на защитата на системата, тъй като тя включва анализа на възможните рискове и заплахи;
- Гарантираност – това е степента на доверие, която може да бъде оказана на архитектурата и реализацията на системата. Тя може да се осъществи чрез тестване или проверки на общия замисъл и изпълнение на системата. Гарантираността е пасивен компонент на защитата, който контролира самите защитни механизми.

Важно средство за гарантиране на сигурността на една система е механизмът на протоколиране. Една надеждна система следва да фиксира всички събития, които засягат сигурността ѝ, както и да извършва одити, т.е анализи на регистрационната информация. Основна задача на надеждната изчислителна база е да изпълнява

функции по мониторинг на заявките, или да се контролира допустимостта за изпълнение от субектите на определени операции над обектите. Реализацията на тази функция представлява ядро на сигурността на информацията, върху което се изграждат всички защитни механизми.

Границата на надеждната изчислителна база е наречена „периметър на сигурност“. От компонентите, които се намират извън този периметър, не се изисква надеждност. С развитието на локални системи, на понятието „периметър на сигурност“ се придава друг смисъл, като се има предвид границата на владение на определената организация. Това, което е вътре в системата, се смята за надеждно, а това, което е извън нея – не. Връзката между вътрешните и външните светове се осъществява чрез „шлюз“, който е създаден с идеята да противостои на потенциално опасна и дори враждебна среда.

Основни елементи на политиката за сигурност

Съгласно „Оранжевата книга“ политиката за сигурност на една система в крайна сметка трябва да включва следните елементи:

Произволно управление на достъпа. Състои се в това, че даден субект от системата (обикновено това е притежателят на обект от системата) може по своя преценка да дава или да отнема на други субекти права на достъп до обекта. Мнозинството операционни системи и системи за управление на бази данни се реализират на този принцип. Главното му достойнство е неговата гъвкавост, а главни недостатъци – децентрализацията и трудният централизиран контрол на достъпите до данни.

Защита от повторно използване на обектите

Това на практика е важно допълнение на средствата за управление на достъпите. Състои се в предпазване от случайно или преднамерено извличане на секретна информация от буферите на системата. Тази защита трябва да се осигури за области от оперативната памет (в частност за буферите с образа на екрана, разшифровани пароли и пр.), за дисковите блокове и за магнитните носители като цяло. Съвременните интелигентни периферни устройства усложняват осигуряването на защитата от повторно използване. И действително принтерът може да буферизира (запамети) някол-

ко страници от документа, които остават в паметта му след приключването на печатането.

Белег (атрибут) за сигурност

За реализацията на принудителното управление на достъпите, със субектите и обектите се асоциират белези за сигурност. Белегът на субекта описва неговата благонадеждност, а този на обекта – степента на секретност на съдържащата се в него информация. Съгласно „Оранжевата книга“ белегът за безопасност се съставя на базата на два компонента: степента на секретност и списъка на категориите. Степента на секретност образува множество, което е в някакъв порядък (например: "Строго секретно'", "Секретно", "Поверително" и "За служебно ползване"), докато категориите образуват непорядъчно множество. Тяхното предназначение е да описват предметната област, към която се отнасят данните. Във военната област всяка категория може да съответства на определен вид оръжие. Този механизъм позволява да се раздели информацията на раздели, което дава възможност за по-добра защитеност. По този начин субектът няма да получи достъп до „чужда“ категория информация дори нивото на неговата благонадеждност да е по-високо.

Един от начините да се осигури ефективност на белега за сигурност, е като се разделят устройствата на многостепенни и едностепенни. На многостепенните може да се работи с информация с ниво на секретност в определен диапазон, а на едностепенните – само с едно ниво. Знаейки нивото на устройството, системата може да реши допустимо ли е да записва на него информация с определен белег. Например опитът да се отпечата информация с ниво на секретност „строго секретно“ на общо използван принтер с ниво „за служебно ползване“, ще претърпи неуспех.

Принудително управление на достъпа

Принудителното управление на достъпа се основава на съпоставянето на белега за сигурност на субекта и на обекта. Този способ се нарича принудителен, защото достъпът не зависи от волята на субекта, нито дори от тази на системния администратор. В зависимост от това как са фиксирани белезите на субекта и обекта, се оказват фиксирани и правата на достъп. Този начин на управление

е реализиран в много операционни системи и системи за управление на бази данни, които се отличават с повишена степен на сигурност. Освен това той е база за начална класификация на информацията и разпределянето на правата за достъп.

Механизъм на отчетност

Този механизъм е допълнение на политиката за сигурност. Неговата цел е във всеки момент от времето да се знае кой работи в системата и какво прави. Това става със следните средства:

Идентификация и автентикация на субекта. Всеки потребител, преди да получи правото да извършва каквото и да е било действие в една система, е длъжен да се идентифицира. Обичаен способ за идентификация е въвеждане на името на потребителя на входа на системата. След като го разпознае, системата е длъжна да провери идентичността на личността на потребителя, т.е. че той е именно онзи, за когото се представя. Стандартно средство за проверка е автентикацията – парола, на принципа на която може да се използват различни видове лични карти, биометрични устройства (сканиране на роговици или отпечатъци от пръсти) или техни комбинации. Това е първото и най-важно програмно-техническо препятствие за информационната сигурност. Без идентификацията на потребителите е невъзможно да бъдат протоколирани техните действия.

Предоставяне на надежден път. Надеждният път свързва потребителя непосредствено с надеждната изчислителна база, елиминирайки други, потенциално опасни компоненти на системата. Целта на предоставянето на път е да даде на потребителя възможност да се убеди в идентичността на обслужващата го система. Реализирането на надежден път е относително просто, когато потребителят се свързва с неинтелигентен терминал, и доста сложно, ако се свързва с интелигентен терминал, персонален компютър или работна станция.

Анализ на регистрационната информация. Одитът има връзка с действия и събития, които имат значение за сигурността за системата. В числото на тези събития се отнасят: влизане в системата; изход от системата; обръщане към отдалечена система; операции с файлове (създаване, закриване, преименуване); смяна на привилегии или други атрибути на защитата (режим на достъп, ниво на

благонадеждност на потребителя и пр.). Ако обаче се фиксират всички събития, обемът на регистрационната информация ще нарасне твърде бързо, а нейният ефективен анализ ще стане невъзможен. „Оранжевата книга“ предвижда наличие на средства за изборно протоколиране както по отношение на потребителите, така и по отношение на събитията.

Протоколирането помага да се следят потребителите и да се възстановяват минали събития, което от своя страна позволява да се анализират случаите на нарушения, да се разбере защо са се случили, да се оценят размерите на щетите и да се вземат мерки за недопускането на подобни щети в бъдеще.

Гарантираност

Гарантираността се разбира като мярка за увереност, с която може да се твърди, че за избраната политика на сигурност е подбран подходящ набор от средства и че всяко от тях правилно изпълнява определената му роля. В „Оранжевата книга“ се разглеждат два вида гарантираност: операционна и технологична. Операционната се отнася до архитектурните и реализационните аспекти на системите, а технологичната – до методите на изграждане и експлоатация на системите. Тя включва проверка на следните елементи:

- Архитектура на системата, която трябва да способства за реализацията на степента на сигурност;
- Цялостност на системата, което в този контекст означава, че програмните и техническите компоненти работят в синхрон;
- Анализ на тайните канали на предаване на информацията – много важна тема за режимните системи, при които главното е да защитят конфиденциална информация. Таен канал се нарича такъв, който не е предназначен за обичайно използване;
- Надеждно администриране. В трактовката на „Оранжевата книга“ това означава да бъдат разделени логически три роли – системен администратор, системен оператор и администратор по сигурността, като физически те може да се изпълняват от един човек, но във всеки момент от времето той може да изпълнява само една от тях;
- Надеждно възстановяване след сривове. Реализацията може да бъде свързана със сериозни технически трудности.

Технологичната гарантираност обхваща целия жизнен цикъл на системата, т.е. периодите на проектиране, реализация, тестване, продажба и експлоатация. Според американските изисквания производителят или продавачът изпълнява набор от тестове, документира го и предоставя резултатите на атестационна комисия, която проверява пълнотата на резултатите. Тестовете трябва да покажат, че защитните механизми функционират в съответствие с описанието си и че не съществуват очевидни начини да се преодолее или разруши защитата.

Документация

Документацията е необходимото условие за гарантиране на надеждността на системата и същевременно инструмент за провеждане на политиката за безопасност. Съгласно „Оранжевата книга“ в комплекта от документи на една надеждна система трябва да присъстват следните части:

- Ръководство на потребителя за средствата за сигурност;
- Ръководство на администратора по защитата;
- Тестова документация;
- Описание на архитектурата.

В „Оранжевата книга“ се определят четири нива на защита на системи: A, B, C и D:

- Ниво D – минимална защита;
- Ниво C – разделна защита;
- Ниво B – мандатна защита;
- Ниво A – верифицирана защита.

Нива B и C са разделени на следните класове: B1 – защита с етикети; B2 – структурна защита; B3 – защитени области; C1 – разделна защита; C2 – защита с управляем достъп. За да може една система след процедури за сертификация да бъде отнесена към едно или друго ниво, нейната политика за сигурност и гарантираност трябва да удовлетворява определени изисквания, които се намират в „Оранжевата книга“.

Критерии за оценка на информационната сигурност в европейските страни

Вървейки по пътя на интеграцията, европейските страни се опитват да унифицират своите критерии за оценка на сигурността

на информационните системи. През 1991 г. са публикувани Information Technology Security Evaluation Criteria, ITSEC.

Принципно важно в европейските критерии е отсъствието на априорни изисквания към условията, в които трябва да работи една информационна система. Организацията, която заявява сертификационни услуги, формулира условията, в които следва да работи системата, възможните заплахи за нейната сигурност и наличните ѝ функции за защита (за разлика от американските критерии, при които има специфични изисквания за условията на правителствените системи, обработващи секретна информация). Задачата на органа по сертифициране е да оцени доколко са постигнати поставените цели, т.е. доколко са коректни и ефективни архитектурата и реализацията на механизма за сигурност в описаните от заявителя условия. Европейските критерии определят следните качества на системата, съставляващи нейната сигурност:

- Конфиденциалност – т.е защита от нерегламентирано получаване на информация;
- Цялостност – защита от нерегламентирана промяна на информацията;
- Достъпност – защита от нерегламентирано притежаване на информация.

При проверката на ефективността на системата се анализира съответствието между целите, формулирани за обекта на защита, и наличния набор от защитни механизми. Способността на механизма на защитата да се противопоставя на преки атаки, се нарича мощност на механизма. Критериите определят три градации на мощността: базова, средна и висока.

Под „коректност на системата“ се разбира правилната реализация на функциите и механизмите на защитата. В критериите се определят седем възможни нива за гарантиране на коректността – от Е0 до Е6, като Е0 е с най-ниска степен. Механизмите за защита се реализират чрез следните функции:

- Идентификация и автентикация – към тези функции се отнасят: проверката на идентичността на потребителя; регистрацията на нови и отпадането на стари потребители; генерирането и изменението на идентификационната регистрация и пр.;
- Управление на достъпите – в този раздел са функции, обезпечаващи временното ограничаване на достъпа, за управление на

правата за достъп и пр.;

- Отчетност – тази функция е аналогична с критериите, заложени в „Оранжевата книга“;
- Одит;
- Повторно използване на обектите;
- Точност на информацията – разбира се като поддържане на съответствие между различни части данни и обезпечаване на неизменност при предаването им;
- Надеждност на обслужването.

В европейските критерии са определени десет класа в зависимост от функциите на защитата на системите. В най-общ вид те съответстват на нивата в „Оранжевата книга“.

Защита от нерегламентиран достъп в Руската федерация

През 1992 г. Държавната техническа комисия при Президента на РФ публикува пет ръководни документа, посветени на проблемите по защита на информацията от нерегламентиран достъп. Поважното от тях е изложено по-долу.

Концепция за защита на средствата на изчислителната техника и автоматизираните системи от нерегламентиран достъп до информацията. Концепцията излага система от възгледи, принципи, които стоят в основата на проблема за защита на информацията от нерегламентиран достъп. В нея са формулирани следните основни принципи на защита:

- Защитата на средствата на изчислителната техника се осигурява от комплекс от програмно-технически средства;
- Защитата на автоматизираните системи се осъществява чрез комплекс от програмно-технически средства и поддържащи ги организационни мерки;
- Защитата на АИС трябва да се осъществява на всички технологични етапи на обработка на информацията и във всички режими на работа, в това число при провеждането на ремонтни и регламентирани дейности;
- Програмно-техническите средства за защита не трябва да се различават съществено по основните си функционални характеристики от тези на АИС;
- Неизбежна част от работата по защита е оценката на ефек-

тивността на средствата за защита, която се прави по методика, отчитаща цялата съвкупност от технически характеристики на оценявания обект;

- Защитата трябва да предвижда контрол на ефективността на средствата за защита от нерегламентиран достъп.

Достъпът до работа с АИС се разделя на четири нива в зависимост от възможностите, които се предоставят на конкретния субект.

Друг ръководен документ на гореспоменатата комисия се нарича *Класификация на автоматизираните системи по нивото на защитеност от нерегламентиран достъп*. Съгласно него се определят девет класа на защита на автоматизираните системи от нерегламентиран достъп до информацията.

Всеки клас се характеризира с определена съвкупност от изисквания по защитата. Класовете се подразделят на три подгрупи, отличаващи се с особености на обработката на информацията в АИС. Във всяка подгрупа се съблюдава йерархия на изискванията по защитата в зависимост от конфиденциалността на информацията, респективно и йерархия в класовете на защитата.

Третата група класифицира автоматизирана система, в която работи само един потребител, който има достъп до цялата информация, намираща се на носители с еднаква степен на секретност. Групата съдържа два класа – 3Б и 3А.

Във втората група потребителите имат еднакви права на достъп до цялата информация, която е с различна степен на секретност. Групата съдържа два класа – 2Б и 2А.

Първата група класифицира АИС, в които едновременно се обработва или съхранява информация с различни нива на секретност и не всички потребители имат еднакви права на достъп. Групата съдържа пет класа – 1Д, 1Г, 1В, 1Б и 1А.

Към различните класове изискванията за защита са различни и са отразени в горепосочения документ, но тъй като са твърде подробни, не смятаме да се спираме върху тях.

ПОЛИТИКА ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ В КОМПЮТЪРНИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ ПРИ БЕДСТВИЯ, АВАРИИ И КАТАСТРОФИ

Общи положения

Защитата на класифицираната информация в компютърните системи за управление при бедствия, аварии и катастрофи засяга всяка автоматизирана система за обработка на информация и управление (АСОИУ), всеки компютър и всички компютърни мрежи, използвани и/или администрирани от дадена организационна единица, в които се създава, обработва, съхранява и пренася класифицирана информация. По-нататък ще наричаме тези системи за управление при бедствия, аварии и катастрофи „АИС или мрежи", така както това е възприето в регулиращите тази материя нормативни документи.

Достъп до класифицирана информация в АИС или мрежи се предоставя само на лица, получили разрешение за достъп, при спазване на принципа „необходимост да се знае", освен ако този закон предвижда друго. Спазването на принципа „необходимост да се знае" се състои в:

1. Ограничаване на достъпа само до определена класифицирана информация;

2. Ограничаване на достъпа само за лица, чиито служебни задължения налагат това;

3. Ограничаване на достъпа само за лица, на които са възложени конкретни задачи, налагащи такъв достъп.

Освен принципа „необходимост да се знае" контекстно приложение намират принципите:

1. Осигуряване на еднаква защита на класифицираната информация, независимо къде и от кого се съхранява;

2. Предоставяне на достъп до класифицирана информация след извършено проучване за надеждност на лицето, което ще ползва достъпа;

3. Отчетност – цялостна регламентация на документалната сигурност на класифицирана информация;

4. Да се знае само колкото е необходимо за изпълнение на преките служебни задължения;

5. Непрекъснато проследяване на движението на класифицирана информация;

6. Съхраняване на толкова класифицирана информация, колкото е необходима за изпълнението на преките служебни задължения.

Сигурността на автоматизираните информационни системи (АИС) или мрежи е система от принципи и мерки за защита от нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в АИС или мрежи. Тя включва прилагане на балансирана система от мерки за сигурност, осигуряващи изпълнението на Задължителни общи условия за сигурност на АИС или мрежи.

Задължителните общи условия за сигурност на АИС или мрежи обхващат компютърната, комуникационната, криптографската, физическата и персоналната сигурност, сигурността на самата информация на всякакъв електронен носител, както и защитата от паразитни електромагнитни излъчвания. Тези условия включват (фиг. 8):

1. Органите по сигурността на АИС или мрежи;

2. Условията и реда за извършването на комплексна оценка на сигурността и издаването на сертификати за АИС или мрежи, наричани по-нататък „акредитиране“;

3. Задължителните общи изисквания за сигурност на АИС или мрежи в областта на (фиг. 9):

а) физическата сигурност;

б) персоналната сигурност;

в) документалната сигурност;

г) комуникационната сигурност;

д) криптографската сигурност;

е) защитата от паразитни електромагнитни излъчвания;

ж) компютърната сигурност.

За всяка АИС или мрежа, в която се създава, обработва, съхранява и пренася класифицирана информация, се изготвят Специфични изисквания за сигурност (СИС). По принцип те се изготвят от длъжностно лице, което в различните държави се нарича по различен начин, но в общия случай то е ръководителят на организационната единица по сигурността на информацията. Тези изисквания подлежат на утвърждаване.

Фиг. 8. *Задължителните общи условия за сигурност*

Фиг. 9. *Задължителните общи изисквания за сигурност на АИС или мрежи*

Специфичните изисквания за сигурност на АИС или мрежи се формулират по време на най-ранния стадий от проектирането на системата и се детайлизират и развиват в процеса на разработването и изпълнението на проекта. Степента на детайлизация зависи от

сложността на системата или мрежата, от режима на сигурност, в който се експлоатира, и от нивото на класификация на обработваната информация. В своя завършен вид СИС определят как се постига, управлява и контролира сигурността на АИС или мрежата.

В отделните етапи на разработка и експлоатация на АИС или мрежата СИС изпълняват различни функции:

1. В етапа на планиране СИС представляват Схематично описание на глобалната и локалната среда за сигурност, в които ще се експлоатира системата, с постепенна детайлизация на изискванията за сигурност;

2. В етапа на разработката или доставката се детайлизират техническите аспекти на СИС, което спомага за правилната спецификация на системата или мрежата;

3. Преди комплексната оценка СИС са в завършен вид и са основа за формулиране на Процедурите за сигурност;

4. В етапа на експлоатация СИС определят границите на отговорност на ОРЕ и на останалия състав, действащ в локалната и глобалната среда за сигурност;

5. В етапа на прекратяване на експлоатацията СИС се ползват за определяне на действията, които трябва да се предприемат с цел запазване на сигурността на информацията.

Специфичните изисквания за сигурност в завършен вид съдържат:

1. Подробно описание на АИС или мрежата по отношение на:

а) формата на представяне и нивото на класификация на информацията;

б) групите потребители според нивото на достъп и начина на взаимодействие със системата;

в) физическата среда за работа;

г) функционалните елементи, включително архитектура, интерфейси и външни връзки;

2. Описание на специфичните заплахи, уязвимостите на АИС или мрежата, режима за сигурност при експлоатация на системата, изискванията към физическата и техническата среда;

3. Описание на глобалната, локалната и електронната среда за сигурност на АИС или мрежата;

4. Подробно описание на мерките за сигурност относно:

а) контрола на достъпа, включително физическия, и определяне на автентичността на потребителите;

б) отчетността на действията на отделните потребители и възможностите за проверка на валидността на тези действия;

в) предотвратяване на възможността за нерегламентиран достъп до информация, включително при повторно използване на обектите на системата;

г) съхраняване на интегритета на информацията;

д) осигуряване на достъпност на информацията;

е) пренасяне на информацията;

ж) други специфични рискове;

5. Управление на сигурността, включително при прилагане на разработените процедури по сигурността, конфигурационния контрол, поддръжката, разработването на документи по сигурността, обучението, случаите, в които се налага допълнително акредитиране;

6. Описание на мерките за сигурност при критични ситуации;

7. Описание на мерките за сигурност при прекратяване на експлоатацията на АИС или мрежата.

При необходимост от по-детайлно разработване на отделните аспекти на сигурността ОАС може да изисква допълнителни СИС за тези аспекти.

Преди въвеждане в експлоатация на АИС или мрежи дирекция, отговорна за това структурна единица от изпълнителната власт, извършва комплексна оценка на сигурността и издава сертификат по образец. Ръководителят на организационната единица, в която се използват АИС или мрежи за обработка на класифицирана информация, по предложение на служителя по сигурността на информацията назначава или възлага на назначени служители от административното звено по сигурността и охраната функции по контрола за спазване на изискванията за сигурност на тези системи или мрежи.

Не се допускат създаване, обработване, съхраняване и пренасяне на класифицирана информация в АИС или мрежи без наличието на издаден сертификат за тези АИС или мрежи. Не се допуска включването на АИС или мрежи, предназначени за създаване, обработка, съхраняване и пренасяне на класифицирана информация, към публични мрежи, като интернет и други подобни електронни комуникационни мрежи.

СИГУРНОСТ НА АИС ИЛИ МРЕЖИ В СИСТЕМАТА ЗА УПРАВЛЕНИЕ ПРИ БЕДСТВИЯ, АВАРИИ И КАТАСТРОФИ

Колективни действия

За да е ефективна системата за информационна сигурност, са необходими общи усилия, включващи участието, разбирането и подкрепата на всички служители, които работят с информация и информационни системи. Поради необходимостта от работа в екип изложената по-долу политика изяснява отговорностите на всички служители и действията, които те трябва да предприемат, за да окажат помощ при защитата на информацията и информационните системи на организацията. В настоящата работа се описват пътищата за предотвратяване и реагиране на различни заплахи за информацията и информационните системи, включително неразрешен достъп, разкриване, размножаване, изменение, присвояване, разрушаване, загубване, злоупотреба и отказ при ползване на информация.

Обхванат персонал

Всички служители на организацията, без значение на техния статус (ръководители, специалисти, консултанти, външни експерти и т.н.), трябва да са запознати, да са съгласни и да изпълняват политиката за информационна сигурност, изложена по-долу. Служителите, които многократно или преднамерено нарушават тези и други положения за информационна сигурност, подлежат на дисциплинарни действия, включително уволнение.

Обхванати системи

Описаната по-долу политика се отнася за всяка автоматизирана система за обработка на информация и управление (АСОИУ), всеки компютър и всички компютърни мрежи, използвани и/или администрирани от организацията, в които се създава, обработва, съхранява и пренася класифицирана информация. Както беше възприето по-горе, наричаме тези системи „АИС или мрежи“ в съответствие с публикуваните държавни (и/или европейски, и/или съюзнически) нормативни документи.

Като начало и с цел конкретизация на изследванията тук ще се

опитаме да дадем още веднъж определение за понятията „автоматизирана информационна система“ и „автоматизирана информационна мрежа“, които по същество не се различават от дадените по-горе прагматични описания на същите тези понятия:

Дефиниция: Автоматизираната информационна система (АИС) е съвкупност от технически и програмни средства, методи, процедури и персонал, организирани за осъществяване на функции по създаването, съхраняването, обработването, ползването и обмена на класифицирана информация в границите на системата. Границите на системата се определят от съответните органи, работещи по сигурността (ОРЕ). Автоматизираната информационна система може да бъде изградена и на основата на една или повече отделни работни станции, несвързани в мрежа, които са в отговорността на ОРЕ.

Дефиниция: Автоматизираната информационна мрежа (или само „мрежа“) е съвкупност от технически и програмни средства, методи и ако е необходимо, персонал и процедури, организирани за осъществяване на обмен на данни (информация) между две или повече АИС или в рамките на една АИС.

Изложената в настоящото изследване политика важи за всички платформи (операционни системи), за компютърни системи от всякакъв вид (от персонални компютри до големи изчислителни машини и суперкомпютри) и всички приложни системи (независимо дали са собствена разработка, или поръчка на външен изпълнител), в които се събира, съхранява, обработва и разпространява класифицирана информация. Тя обхваща само такива компютри и/или мрежи. Даже ако в настоящата работа се споменава друго (например гласово и писмено разпространение на информация), то не е пряко адресирано към сигурността на информацията извън тези АИС или мрежи. Както беше отбелязано по-горе, съгласно българското законодателство класифицирана информация е „информацията, представляваща държавна или служебна тайна, както и чуждестранната класифицирана информация“.

Дефиниция: Глобална среда за сигурност на АИС или мрежата е средата, в която е разположена АИС или мрежата и в която са приложени мерки за физическа, персонална и документална сигурност, които са в отговорността на служителя по сигурността на информацията на организационната единица и са извън контрола на ОРЕ.

Дефиниция: Локална среда за сигурност на АИС или мрежата е средата, в която е разположена АИС или мрежата и в която са приложени мерки за физическа, персонална и документална сигурност, които са в отговорността на органа по развитие и експлоатация на АИС или мрежи (ОРЕ).

Дефиниция: Обект на АИС или мрежа (или само „обект“) е пасивен елемент на АИС или мрежата, който съдържа или приема информация.

Дефиниция: Субект на АИС или мрежа (или само „субект“) е активен елемент на АИС или мрежата (лице, процес или устройство), който осъществява обмен на информация между обектите или изменение в състоянието на системата или мрежата.

Дефиниция: Създаване, обработване, съхраняване или предоставяне на класифицирана информация е създаването, маркирането, регистрирането, съхраняването, ползването, предоставянето, трансформирането и разсекретяването на класифицирана информация.

Органи, работещи по информационната сигурност. Базова постановка

Органите, работещи по информационната сигурност, са показани на фиг. 10.

Ръководителят на организационната единица ръководи, организира и контролира дейността по защита на класифицираната информация. Той е отговорен за създаването, установяването и поддръжката на политиката (стратегията) за защита на класифицираната информация и в частност за внедряването на стандартите, ръководствата и процедурите, засягащи цялата организация.

Ръководителят на организационната единица (РОЕ) назначава служител по сигурността на информацията след получаване на разрешение за достъп на това лице до класифицирана информация, издадено от съответния орган. По изключение, в зависимост от нивото и обема на класифицираната информация, ръководителят на организационната единица може да изпълнява функциите на служител по сигурността на информацията, ако отговаря на описаните в закона изисквания. Служителят по сигурността на информацията е пряко подчинен на ръководителя на организационната единица.

Фиг. 10. *Органи, работещи по информационната сигурност*

По принцип и в съответствие с дадените от законодателя пълномощия:

Държавните органи по сигурността на информацията осъществяват общ контрол: (1) по защита на класифицираната информация, съхранявана, обработвана и пренасяна в АИС или мрежи; (2) на процеса на акредитиране на АИС или мрежи.

Ръководителят на организационната единица, в която се експлоатират или се предвижда изграждането на АИС или мрежи за обработка на класифицирана информация, по предложение на служителя по сигурността на информацията назначава в административното звено по сигурността служител по сигурността на АИС или мрежи или възлага на назначени служители от същото звено неговите функции.

Служителят по сигурността на АИС или мрежи е отговорен за установяването на политиката за сигурност на АИС или мрежи в организационната единица. Той определя изискванията за сигурност към АИС или мрежи, произтичащи от общата политика за сигурност на организационната единица, координира изготвянето на специфичните изисквания за сигурност на АИС или мрежи, процедурите за си-

гурност и на изработените на тяхната основа експлоатационни документи по сигурността координира обучението по сигурността на АИС или мрежи, осъществява контрол за спазване на изискванията за сигурност, разследва обстоятелствата, свързани с компрометиране на сигурността, и докладва за резултатите на служителя по сигурността на информацията в организационната единица, който уведомява Органа по акредитиране на сигурността (ОАС).

Органът по развитие и експлоатация на АИС или мрежи в организационната единица:

1. Участва в определянето на политиката за сигурност на АИС или мрежи в организационната единица;

2. Изготвя документите по сигурността на АИС или мрежата;

3. Осигурява изпълнението на изискванията за акредитиране на АИС или мрежи и прави заявки за допълнително акредитиране на АИС или мрежата, когато това е необходимо;

4. Участва в определянето на мерките за сигурност и границите на отговорност при осъществяването на връзки с други АИС или мрежи;

5. Прави предложение за възлагане на функции на администратор по сигурността на АИС или мрежата и осигурява подготовката му;

6. Организира и провежда обучение по сигурността в АИС или мрежи на служителите в Органа по развитие и експлоатация (ОРЕ) и на потребителите на АИС или мрежата;

7. Прилага одобрените мерки за сигурност в АИС или мрежата;

8. Прави преглед на свързаната със сигурността документация периодично или при предложени промени в техническото или програмното осигуряване, връзките с други АИС или мрежи, режима за сигурност, нивото на класификация на информацията или при други дейности, които могат да повлияят на сигурността на АИС или мрежата, като за резултатите информира служителя по сигурността на АИС или мрежи;

9. Участва заедно със служителя по сигурността на АИС или мрежи в установяването на обстоятелствата, свързани с компрометиране на сигурността на АИС или мрежи.

Със заповед на ръководителя на организационната единица, по предложение на ОРЕ, съгласувано със служителя по сигурността на информацията, се възлагат функции на администратор по си-

гурността на АИС или мрежата. Той е от състава на ОРЕ или от друго звено в организационната единица, имаща отношение към АИС или мрежата. При необходимост може да се определят повече от един администратор по сигурността, отговарящи за обособени части, като един от тях се определя за администратор по сигурността на цялата АИС или мрежа. Задълженията на администратора по сигурността на АИС или мрежата и на администратора на АИС или мрежата трябва да са ясно разграничени.

Администраторът по сигурността на АИС или мрежата трябва да има разрешение за достъп до най-високото ниво на класифицирана информация в АИС или мрежата. Когато автоматизираната мрежа обхваща няколко организационни единици, всяка от тях определя администратор по сигурността за своята част от мрежата.

Администраторът по сигурността на АИС или мрежата:

1. Участва в изготвянето и актуализирането на процедурите по сигурността на АИС или мрежата;

2. Изготвя експлоатационни документи по сигурността на АИС или мрежата за обслужващия персонал и потребителите на базата на утвърдените процедури за сигурност;

3. Изпълнява възложените му процедури за сигурност в АИС или мрежата;

4. Периодично информира обслужващия персонал и потребителите по въпросите на сигурността на АИС или мрежата;

5. Осигурява на потребителите достъп до ресурсите на АИС или мрежата в съответствие с предоставените им права;

6. Осъществява пряк контрол по отношение на изпълнението на мерките и процедурите за сигурност в АИС или мрежата, като:

а) следи за спазването на мерките и процедурите за сигурност в зоните за сигурност на АИС или мрежата;

б) следи за спазването на мерките и процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в АИС или мрежата;

в) следи за правилното функциониране на механизмите за сигурност;

г) управлява, наблюдава и анализира свързаните със сигурността одитни записи на системата и при констатиране или при съмнения за компрометиране на сигурността докладва на ОРЕ и на служителя по сигурността на АИС или мрежи;

д) осигурява резервиране и съхраняване на одитните записи в определените срокове;

7. Участва заедно със служителя по сигурността на АИС или мрежи и с ОРЕ в установяването на обстоятелствата, свързани с компрометирането на сигурността на АИС или мрежата;

8. Изпълнява функциите на администратор по криптографска защита на информацията, ако в АИС или мрежата се прилагат криптографски методи и средства.

Потребител на АИС или мрежата е лице, което:

1. има издадено разрешение за достъп до най-високото ниво на класификация за сигурност на информацията, с която има право да работи в АИС или мрежата;

2. е преминало обучение в областта на сигурността на АИС или мрежа;

3. е с предоставени права за достъп до ресурсите на АИС или мрежа.

Потребителите в АИС или мрежа изпълняват задълженията, посочени в експлоатационните документи по сигурността на АИС или мрежа. Те изпълняват указанията на администратора по сигурността на АИС или мрежа, свързани със сигурността на системата или мрежата, и уведомяват администратора по сигурността за всички случаи или съмнения за компрометиране на сигурността на АИС или мрежата.

Класифицирана информация

Както беше отбелязано по-горе, в общия случай можем да приемем, че **класифицирана информация е информацията, представляваща държавна или служебна тайна, както и предоставената или придобита чуждестранна класифицирана информация**. Държавните субекти формулират Списък на категориите информация, подлежащи на класификация като държавна тайна.

Държавна тайна е информацията, определена в този списък. Нерегламентираният достъп до нея би създал опасност за или би увредил интересите на съответната държава, свързани с националната ѝ сигурност, отбраната, външната политика или защитата на конституционно установения ред.

В общия случай служебна тайна е информацията, създавана или съхранявана от държавните органи или органите на местното

самоуправление, която не е държавна тайна, нерегламентираният достъп до която би се отразил неблагоприятно на интересите на държавата или би увредил друг правнозащитен интерес. Информацията, подлежаща на класификация като служебна тайна, се определя със закон. Съответно ръководителят на организационната единица обявява със заповед списъка на категориите информация, подлежащи на класификация като служебна тайна.

Ръководителят на съответната организационна единица в рамките на съответен законов регламент обявява списък на категориите информация за сферата на дейност на организационната единица. Чуждестранна класифицирана информация е класифицираната информация, предоставена и/или придобита от друга държава или международна организация.

Класифициране на информацията е дейност, при която се установява:

1. попада ли конкретната информация в списъка на категориите съответна информация;

2. налице ли е заплаха или опасност от „увреждане“ на самата информация или увреждане в съответната степен на нечии интереси;

3. дали нерегламентираният достъп до нея би създал опасност за интересите по т. 1;

4. налице ли са обществените интереси, подлежащи на защита.

Информацията се класифицира според собственото ѝ съдържание, а не според класификацията на информацията, на която се базира, или информацията, за която се отнася.

Нива на класификация за сигурност на информацията

Нивата на класификация за сигурност на информацията и техните грифове за сигурност в различните държави и в общия случай може да се сведат до следните: „Строго секретно“, „Секретно“, „Поверително“, „За служебно ползване“ и др. (понякога се прави допълнителна класификация за информация от ИЗКЛЮЧИТЕЛНА ВАЖНОСТ).

Информацията, класифицирана като държавна тайна, се маркира с гриф за сигурност:

„Строго секретно“ – в случаите, когато нерегламентиран достъп би застрашил в изключително висока степен суверенитета на

дадена страна, нейната независимост, териториалната ѝ цялост или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на непоправими или изключително големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред;

„Секретно“ – в случаите, когато нерегламентиран достъп би застрашил във висока степен суверенитета на дадена страна, нейната независимост, териториалната ѝ цялост или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на трудно поправими или големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред;

„Поверително“ – в случаите, когато нерегламентиран достъп би застрашил суверенитета на дадена страна, нейната независимост, териториалната ѝ цялост или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред;

„За служебно ползване“ – информацията, класифицирана като служебна тайна.

С цел осигуряване на допълнителна защита, когато това се налага от характера на информацията или когато е предвидено в международни договори, по предложение на съответния оторизиран орган може да се определят с решение:

1. Допълнителни маркировки на материали и документи с по-високо ниво на класификация от „Строго секретно“;

2. Специален ред за създаване, ползване, размножаване, предоставяне и съхраняване на тези материали и документи;

3. Кръгът на лицата с право на достъп до тези материали и документи.

Приравняването на нивата на класификация за сигурност на получаваната чуждестранна класифицирана информация или на предоставяна на друга държава или международна организация та-

кава информация в изпълнение на влязъл в сила международен договор за дадена страна и за съответната чужда държава или международна организация се осъществява в съответствие с разпоредбите на договора.

Ръководителят на съответната организационна единица обявява със заповед списъка на категориите информация, подлежащи на класификация като служебна тайна. Ръководител на държавен орган, управляващ правата на собственост на държавата в организационни единици – търговски дружества с повече от 51% държавно участие, обявява със заповед общия списък на категориите класифицирана информация, съставляваща служебна тайна за отрасъла, подотрасъла или търговската дейност. Този списък съдържа само категории информация, създавана, обработвана и съхранявана в организационната единица, определени като тайна в специални закони.

Ръководителят на организационната единица определя със заповед списък на длъжностите или задачите, за които се изисква достъп до класифицирана информация, представляваща служебна тайна.

Маркиране, съхраняване и защита на информацията

Ръководителите на организационните единици организират обучението на подчинените им служители за условията и реда за маркиране на информацията (поставянето, промяната и заличаването на грифовете за сигурност).

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИ АСПЕКТИ НА ЗАЩИТАТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ В АИС ИЛИ МРЕЖИ

Тук ще направим опит да представим модел на защитата на класифицираната информация, създавана, обработвана, съхранявана и пренасяна в АИС или мрежа в системата за управление при бедствия, аварии и катастрофи.

Специфичните и общите изисквания за сигурност са основата, върху която се базират всички действия по защитата на класифицираната информация. Те са ориентирани към производителите и органите по сертифициране на системите и мрежите, не отчитат

постоянната необходимост от промяна на защитаваните обекти и не съдържат практически правила за защита на информацията. Информационната сигурност не се купува. Тя се поддържа ежедневно от хората. Стандартите и нормативните изисквания не дават отговор на въпросите:

- Как да се изгради сигурна информационна система?
- Как да се организира и поддържа защитата в постоянно променяща се среда и структура на системата?

Управленски мерки за защита на класифицираната информация в АИС или мрежи

Главната цел на мерките, предприети на управленско ниво, е да се сформира програма за работа в организационната единица по отношение на информационната сигурност, да се осигури изпълнението, като се отделят необходимите ресурси и се осъществява последващ контрол. Основа на тази програма е политиката за сигурност, която отразява подхода на организационната единица към защитата на нейните информационни масиви.

Политика за информационна сигурност

Политиката за информационна сигурност е съвкупност от закони, принципи, правила и норми на поведение, определящи методите и средствата за вземане на решения за защитата на класифицираната информация в процесите на нейното създаване, обработка, съхранение, ползване и обмен, в границите на дадената система. В частност правилата определят кога потребителят може да работи с определени данни. Колкото по-надеждна е дадена информационна система, толкова по-дисциплиниращa и разнообразна е политиката за сигурност. В зависимост от формулираната политика се избират конкретните методи и средства за гарантирането на сигурността ѝ.

Политиката за информационна сигурност е активен компонент на защитата, включващ резултатите от анализа на възможните заплахи, сценарии за реализацията им, оценка на риска и избор на методи и средства за противодействие. Тя поддържа интересите на субектите на автоматизираните информационни системи и мрежи и допринася за постигането на техните цели.

Политиката за информационна сигурност не е самоцелна или

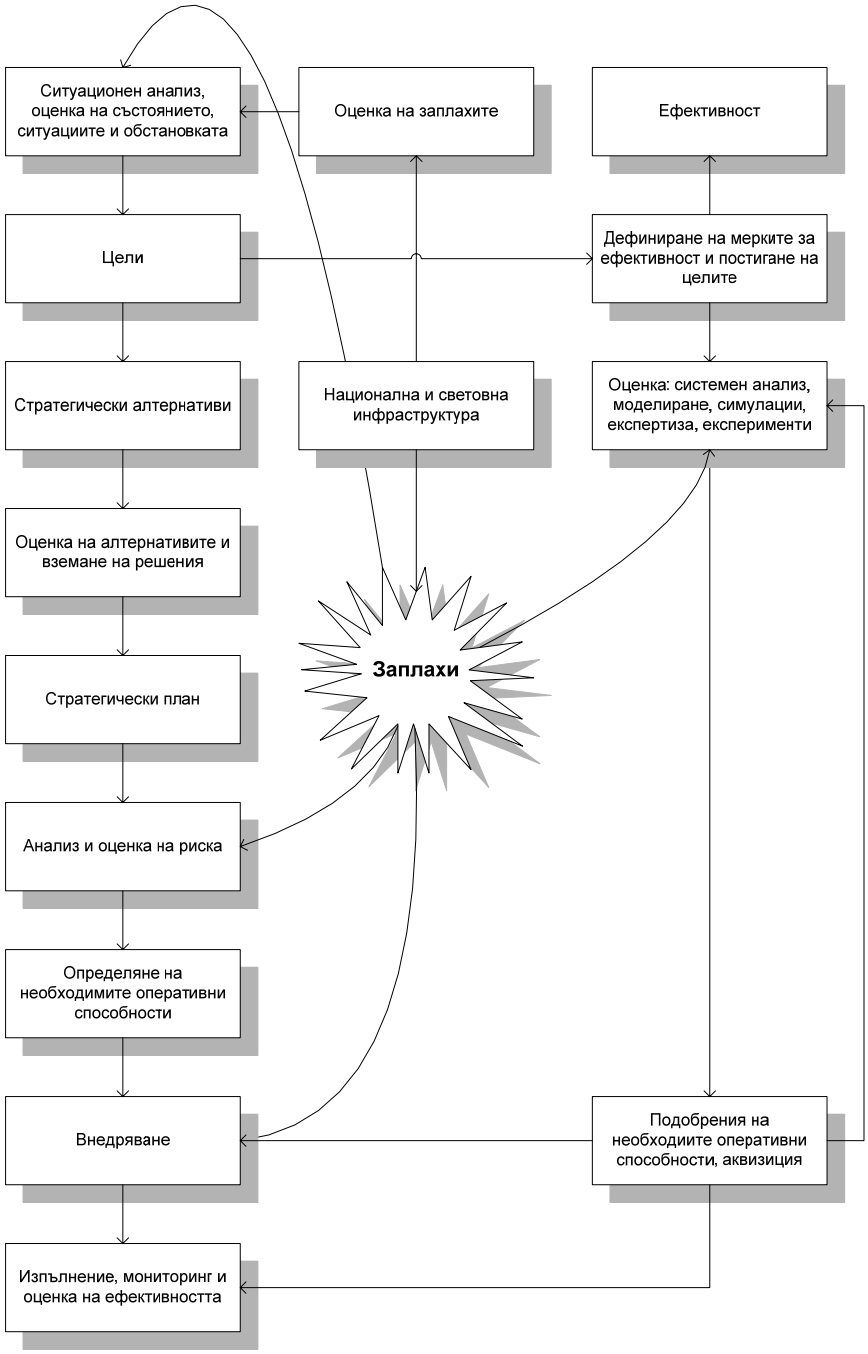
рефлексивна проява по отношение на някакви заплахи. Тя включва система (комплекс) от знания и технологии за рационално използване на информационните инфраструктури и ресурси със стратегическа цел – защита на жизненоважните интереси на личността, обществото и държавата от заплахи в информационното пространство. На стратегическо равнище тези интереси включват:

- Опазване на националния суверенитет в националното информационно пространство;
- Създаване на благоприятни условия за материално, духовно и интелектуално процъфтяване на нацията;
- Развитие на националния научен и образователен потенциал и разцвет на националната култура.

Оперативната цел на тази политика е да се подобри защитеността на класифицираната информация в рамките на държавния суверенитет, при спазване на конституционното право на всеки субект да търси, получава и разпространява информация. Осъществяването на това право може да се ограничава дотолкова, доколкото не може да бъде насочено срещу правата и доброто име на други граждани, както и срещу националната сигурност, обществения ред, народното здраве и морал.

По своята същност провеждането на политика за информационна сигурност е държавна дейност, произтичаща от възприетия общополитически курс, осигуряващ най-благоприятни условия за развитие на обществото, държавата, личността и гарантиращ националните интереси в информационното пространство чрез установяването на оптимално съотношение между структурните елементи на сигурността. За да реализират политиката за информационна сигурност, субектите на изпълнителната, законодателната и съдебната функция на държавната власт все повече се нуждаят от ефективни инфраструктури за съхранение, обработка и пренасяне на критична информация за нуждите на планирането, ръководството, координацията и контрола на текущите си дейности (виж фиг. 11).

В тези инфраструктури има множество уязвими места, които може да бъдат атакувани и разрушени от специфични сили с голяма информационна мощ.



Фиг. 11. *Заплахи*

В началото на XXI век това се превърна в една от най-сериозните заплахи за националната сигурност на страната. Ускореното внедряване на информационни технологии ще води до все по-засилваща се зависимост на отделната личност, обществото и държавата от тях. Това разширява възможностите за употреба на информационни средства за насилие, т.е. засилва инфраструктурната уязвимост на обществото. Тази уязвимост разкрива нови възможности за постигане на крайни политически цели чрез нанасяне на неприемлив ущърб на информационното пространство, което досега не се смяташе за област със стратегически рискове и заплахи. Увеличаването на значението на информационния компонент на сигурността налага да се разработи ефективна политика за акумулиране и използване на информационна мощ с цел отразяване на заплахите в информационното пространство.

От практическа гледна точка политиката за сигурност може да се раздели на три нива.

Към политиката за информационна сигурност на високо (стратегическо) ниво може да се отнесат решения, които имат отношение към цялата организация. Те се вземат от ръководството на организацията и са с по-общ характер, като например:

- Решение да се проектира или преразгледа комплексна програма за защита на информацията;
- Решение да се формулират целите, които организацията преследва в областта на защитата на класифицираната информация;
- Решение да се осигури база за спазване на законите и наредбите;
- Решение да се систематизират управленските решения по въпросите за реализация на програмите за защита, които са валидни за цялата организация.

Целите на организацията в областта на информационната сигурност на това първо ниво се формулират с термините **конфиденциалност, достъпност** и **интегритет**. Към това ниво на управление се отнасят защитата на ресурсите и координацията при използването на тези ресурси, обособяването на специален персонал за защита на критично важни системи, поддържането на контактите с други организации и пр.

Политиката за сигурност от това ниво има връзка с три аспекта

на законосъобразност и изпълнителска дисциплина. Първо, организационната единица е длъжна да спазва съществуващите закони. Второ, трябва да контролира действията на лицата, които отговарят за изработването на програмите за сигурност. И накрая, необходимо е да се осигури определена степен на отговорност на персонала.

Политиката за информационна сигурност на средно (оперативно) ниво засяга въпроси, които имат отношение към отделни аспекти на защитата на информацията. Примери за такива въпроси са достъпът до интернет (как да се съчетае правото да получаваш информация, със защитата от външни заплахи), използването от потребителите на неофициално програмно осигуряване и т.н. Политиката за сигурност на това ниво има отношение към изброените по-долу теми:

Описание на аспекта. Под „описание на аспекта“ се разбира описанието на заданието за конкретните изисквания към мрежата, с каква информация ще се работи, с какви ресурси се разполага, на какви изисквания за защита трябва да отговори системата и т.н.

Обхватът и нивото на сигурността на мрежата зависят от конкретната работна среда. Например за мрежа, съхраняваща данните на важно държавно учреждение, трябва има по-висока степен на защита, отколкото за мрежа, обединяваща компютрите на една малка фирма. Въпреки това мрежовата сигурност изисква изчерпателен набор от правила и политики за сигурност, съставен така, че нищо да не бъде оставено на случайността.

Сфера на използване. Отговаря на въпросите: къде, кога, как, по отношение на кого и какво се приема дадената политика за сигурност.

Позиция на организацията по дадения аспект. Към тази тема може да се отнесат целите на организацията по отношение на защитата на класифицираната информация. Най-добрите политики за сигурност на данните използват превантивния подход. Чрез предотвратяване на възможността за неоторизиран достъп данните ще останат защитени.

Права и задължения на лицата, отговарящи за провеждането на политиката за сигурност. Тези права и задължения се определят със Закона за защита на класифицираната информация и съпътстващите го поднормативни документи. Политиките определят на-

соките и правилата, които могат да бъдат от полза на администраторите и потребителите при възникването на непредвидени ситуации в мрежата. Например, ако трябва да се проверяват дискети от друг компютър, е необходимо да се опишат процедурите за проверка. Ако не трябва да се използват неофициални програмни продукти, е необходимо да се знае кой отговаря за изпълнението за това правило и т.н. Най-общо групите хора, които имат отношение към сигурността на информацията в една система или мрежа, са: ръководителите, системните инженери, системните администратори, системните организатори и потребителите. Техните права и задължения може накратко да се опишат, както следва:

• Ръководителят трябва да държи в полезрението си въпросите по защитата на информацията; да контролира действията на подчинените си по този въпрос; да отчита рисковете и заплахите; да информира администраторите за всяка промяна на статуса на работниците – смяна на длъжност, уволнение и пр.;

• Администраторът на мрежата трябва ежедневно да следи и анализира информацията, отнасяща се за мрежата като цяло; да информира ръководството за ефективността на съществуващата политика за сигурност, както и за опити да бъде нарушена защитата; периодично да извършва проверки за надеждността на защитата на локалната мрежа и т.н.;

• Потребителите от своя страна трябва да се запознаят и да спазват законовите разпоредби и вътрешноведомствените правила на политиката за сигурност, да използват достъпни защитни механизми за осигуряване на конфиденциалността на своята лична информация, да знаят слабостите, които се използват за нерегламентиран достъп и „проникване“ в системата, да следят за такива опити и своевременно да информират компетентните лица, и пр.

Законосъобразност. Политиката за сигурност на една организация трябва да съдържа общо описание на забранените действия и наказанията за тях. Случаите на нарушения от страна на персонала трябва да се разглеждат от ръководството и да се предприемат наказателни мерки, включително уволнение.

При определяне на политиката за сигурност трябва да се знае към кого може да се обръщаме за разяснение, помощ и допълнителна информация.

Политиката за сигурност на най-ниско (тактическо) ниво зася-

га конкретното програмно осигуряване. За разлика от предишните две нива тя е доста по-детайлна. Ето няколко примера за въпроси, на които трябва да се отговори при определянето на политиката за сигурност на това ниво:

- При какви условия може да се четат и изменят данните в информационната система?
- Кой има право на достъп до обектите, поддържащи програмното осигуряване?

Формулирането на целите на политиката на най-ниското ниво може да се основава на съображенията за конфиденциалност, достъпност и цялостност, но тези цели трябва да бъдат конкретно формулирани.

От целите произтичат правила за защита на информацията, описващи кой, какво и при какви условия може да върши. Колкото по-детайлни са правилата, толкова по-лесно е да се изпълняват програмно-техническите изисквания. От друга страна, много строгите правила може да пречат на работата на потребителите. Затова ръководството трябва да намери разумен компромис, при който за приемлива цена може да се осигури приемливо ниво на защита, без да се ограничават служителите.

Програма за защита на информацията

След като се определи политиката за сигурност на една система, може да се пристъпи към изготвянето на програма за защита на информацията и към нейното реализиране. Програмата може да се структурира също на отделни нива, съответстващи на структурата на самата организация. Най-често са достатъчни две нива: централно и изпълнителско.

Програмата на централно ниво се отнася за цялата организация и може да се ръководи от лицето, отговарящо за сигурността на информацията в АИС или мрежи, като главните ѝ цели са:

- оценка на рисковете и заплахите, избор на ефективни средства за защита;
- координация на дейностите на различните отдели и служители при защитата на информацията;
- стратегическо планиране;
- контрол на дейностите в областта на защитата на класифицираната информация.

Тук може да се отчете фактът, че информационните технологии се развиват много бързо, и затова в тази програма е необходимо да се заложи и внедряването на нови средства.

Контролът на дейностите в областта на защитата на информацията е в две направления. Едното е насочено към външни, контролиращи организации, за да се гарантира, че действията на организацията не противоречат на закона. Другото направление е насочено навътре към самата организация, за да може да се реагира в случаи на нарушения и да се актуализират мерките за защита в зависимост от промяната на обстановката.

Целта на програмата на изпълнителско ниво е да осигури надеждна и икономична защита. На това ниво се решава какви механизми на защита може да се използват, закупуването и установяването на технически средства и т.н. За изпълнението на действията по програмата трябва да отговаря администраторът на мрежата.

Програмата за сигурност не бива да се превръща в набор от технически средства, построени в система, защото така ще загуби своята независимост и авторитет и като следствие висшето ръководство ще забрави за нея.

Управление на риска

На трето, но не и на последно място от управленските мерки за защита на класифицираната информация е управлението на риска. Дейностите на една организация, работеща с класифицирана информация, са изложени на много рискове, още повече когато тази информация се разпространява по АИС или мрежа.

Работата по управление на риска се състои в това да се оцени неговият размер, да се изготвят мерки за намаляването му и да се придобие увереност, че рискът е ограничен до приемливи размери.

Първата стъпка е избор на анализируем обект. За неголеми организации може да се разглежда цялата информационна инфраструктура, но за крупни организации това може да се окаже необосновано скъпо и бавно. В тези случаи ще трябва да се анализират най-важните възли от мрежата. Уязвими места може да се появят на всички места от информационната система – от мрежовия кабел, който може да бъде прегризан от мишки, до базата данни, която може да бъде разрушена от неумелите действия на администратора. Много е важно да се избере разумна методология за оценка на

риска. Целта на оценката е да се получи отговор на два въпроса: Приемливи ли са съществуващите рискове? Ако не, какви защитни средства е икономически изгодно да използваме? Оценката е количествена. Управлението на риска е типична оптимизационна задача и съществуват достатъчно програмни средства, които могат да помогнат да бъде решена.

Когато анализируеми обекти са класифицираната информация, компонентите на информационната система, програмните ресурси, поддържащата инфраструктура и персоналът, трябва да се класифицират данните по ниво на секретност, да се определят местата за съхранение и обработка и начините за достъп до тях. Важно е да се систематизират обектите, за да може да се направи оценка за последствията от нарушаването на защитата на информацията.

Рискът се появява там, където има заплаха. Кратък преглед на най-разпространените заплахи показва, че те са много и не всички имат отношение към компютърните системи или мрежи. Като правило, наличието на една или друга заплаха е следствие на слабости в защитата на информационната система, което се обяснява с отсъствието на някои програмно-технически средства за сигурност или с недостатъци в реализиращите ги защитни механизми. В примера с прегризания от мишки кабел заплахата идва не от съществуването на мишки, а от отсъствието или недостатъчната дебелина на защитната обвивка на кабела.

При определянето на заплахите за класифицираната информация в автоматизираните информационни системи и мрежи първата стъпка е идентификацията. Анализируемите видове заплахи следва да се избират на базата на здравия разум (като оставим настрана например заплахата от земетресение и други природни бедствия), но в рамките на избраните видове заплахи трябва да се направи максимално пълен анализ. Целесъобразно е да се определят не само самите заплахи, но и източниците им. Това може да помогне при избора на допълнителни средства за защита.

След идентификацията на заплахите е необходимо да се оцени вероятността за осъществяването им. Може да се използва тристепенна скала: ниска, средна и висока вероятност. Освен вероятността за осъществяване важен е и потенциалният размер на щетите (също висок, среден и нисък). Например пожари се случват рядко, но размерът на щетите от тях е голям и т.н. При оценяването на

заплахите трябва да се изхожда не само от средностатистическите данни, но и да се отчитат специфичните особености на конкретната информационна система, организационна единица и персонал.

Следващата стъпка е оценката на риска. Може да се използва такъв прост метод като умножение на вероятността за осъществяване на заплаха и предполагаемите щети. Възможните варианти са нисък, среден и висок риск. По тази скала може да се оцени приемливостта на риска и съответно, ако някои рискове се окажат неприемливо високи, се реализират допълнителни мерки за защита.

За премахването на слабости, създаващи реална опасност, съществуват механизми, отличаващи се с голяма степен на ефективност. Например, ако има голяма опасност от нерегламентирано проникване в системата, може да се задължат потребителите с достъп да избират дълги пароли, да задействат програма за генериране на пароли или да закупят интегрирана система за автентикация на основата на интелектуални карти.

При оценяването на стойността на защитните мерки е необходимо да се отчитат не само средствата, които ще са необходими за закупуването на оборудването и програмите, но и разходите за внедряването, поддръжката, обучението и преквалификацията на персонала. Ако по този показател новото средство се окаже икономически изгодно, може да бъде допуснато за по-нататъшно разглеждане.

Когато необходимите мерки са приети, трябва да се провери тяхната действеност, т.е. да се постигне убеденост, че остатъчният риск е станал приемлив. Ако това е така, може да започне процедурата по сертификация според действащото законодателство. Ако не, се анализират допуснатите грешки и се провежда повторен сеанс на управление на риска.

Сигурност на жизнения цикъл на системата

Жизненият цикъл на системата може да се раздели на следните етапи:

Стартиране. На този етап се оформя разбирането за това, че е необходимо да се придобие нов (или значително да се модернизира съществуващ) продукт. Изготвят се задания с характеристики и функции, които трябва да притежава продуктът. Оценяват се финансовите и други ограничения. На всеки от етапите се отчита фактът, че в системата ще се обработва класифицирана информа-

ция. Необходимо е да се направи оценка на критичността на самата система, от която зависи степента на внимание, което службата за сигурност на организационната единица трябва да отдели на системата през следващите етапи от жизнения ѝ цикъл.

Покупка. Това е най-трудният етап. Трябва окончателно да се формулират изискванията към средствата за защита на новата система, към фирмата, която ще монтира системата, към квалификацията на персонала и пр. Всички тези сведения се оформят в спецификация, където влизат документацията, сервизното обслужване, обучението на персонала и др. Особено внимание трябва да се обърне на въпроса за съвместимостта на новата система с наличните конфигурации. Трябва да се отбележи, че нерядко средствата за защита са незадължителни компоненти на търговските продукти и е необходимо да се проследи дали съответните пунктове не са отпаднали от сертификацията.

Монтаж. Това е етапът, при който новата система се установява, конфигурира, тества и въвежда в експлоатация.

Експлоатация. Това е най-дългият и сложен процес. Най-голяма заплаха за информацията има през този етап. Ако сигурността на една система не се поддържа, тя има свойството да отслабва. Потребителите не държат ревностно да изпълняват инструкциите, администраторите анализират регистрираната информация с по-малка бдителност. Ту един, ту друг потребител получава допълнителни привилегии. На пръв поглед нищо не се изменя, но на практика защитата на информацията намалява. За борба с ефекта на „бавните изменения“ трябва да се прибегне до периодични проверки на сигурността на системата за защита.

Извеждане от експлоатация. В нашия случай, говорейки за АИС или мрежи, в които се обработва класифицирана информация, при извеждане на системата от експлоатация трябва да се унищожават физически апаратните компоненти, носители на такава информация.

Организационни мерки за защита на класифицираната информация в АИС или мрежи

Тези мерки са ориентирани към хората. Именно те формират режима на защита и те се оказват главната заплаха. Затова човешкият фактор заслужава първостепенно внимание.

Управление на персонала

Управлението на персонала започва с приемането на служителя на работа и дори преди това – при съставянето на длъжностна характеристика. Още на този етап е необходимо да се привлече специалист по защита на информацията, който да определи компютърните привилегии, асоцируеми с длъжността. При управлението на персонала съществуват два принципа, които трябва да се вземат под внимание:

Разделение на отговорностите. Според този принцип ролите и отговорностите се разпределят така, че един човек да не може да наруши критически важен за организационната единица процес.

Минимизация на привилегиите. Той предписва как да се дават на потребителите само тези права на достъп, които са им необходими за изпълнение на служебните задължения.

В действащата нормативна база много подробно и категорично са определени критериите за издаване на разрешение на лице за работа с класифицирана информация. Кандидатите се проверяват щателно от съответните служби за сигурност, извършват се проверки, беседи, за да не се допусне назначаване на лица, извършили престъпления, душевно болни или ненадеждни от гледна точка на опазване на тайната. Процедурата е дълга и зависи от нивото на класификация на информацията за достъп, за което кандидатства лицето.

Когато кандидатът е одобрен, той трябва да премине обучение, да бъде запознат с нормативната база и да му бъде проведен изпит по защита на класифицираната информация. Желателно е, а и законът го изисква, тези процедури да са извършени преди встъпването на служителя в длъжност и преди той да бъде включен в списъка с входящи имена, пароли и допуски. След този момент започват неговото администриране, протоколиране и анализът на неговите действия като потребител.

Когато един потребител напусне организацията, особено в случаи на конфликт между сътрудника и организацията, е необходимо да се действа максимално оперативно. Възможно е и физическо ограничаване на достъпа до работното място.

Понякога обслужването и администрирането на компоненти на компютърната система се поемат от външни организации. Това създава допълнителни слабости в защитата, които е необходимо да се компенсират със засилен контрол на достъпа или обучение на

собствени служители. Проблемът за обучението на персонала е един от основните, що се отнася до защитата на информация. Ако служителят не е запознат с политиката за сигурност, той не може да се стреми към постигането на формираните цели. Ако не знае мерките за сигурност, той не може да ги съблюдава. Напротив, ако знае, че неговите действия се контролират, е възможно да се въздържи от нарушение. Обучението трябва да се провежда редовно и всеки път по различен начин, иначе ще се превърне във формалност и ще загуби своята ефективност.

Физическа защита

Сигурността на АИС или мрежи зависи от обкръжението, в което работят, следователно необходимо е да се предприемат мерки за защитата на сградите и прилежащите територии, поддържащи инфраструктурата и самите компютри.

В действащото законодателство съществува много добра нормативна база по отношение на физическата защита на класифицираната информация. Това са Законът за защита на класифицираната информация и Наредбата за физическа защита.

Мерките за физическото управление на достъпа позволяват да се контролират и при необходимост да се ограничават влизането и излизането на служители и посетители. Може да се контролира цялата сграда на организацията, както и отделни помещения, например тези, в които са разположени комуникационната апаратура и сървърите (*във всички законови уредби и подзаконови актове те са определени като зони за сигурност*). Средствата за физическа защита са известни отдавна. Това са: охрана, прегради, видеонаблюдение, обемни детектори и др. Важно е да се разграничат компютрите и потокът от посетители или в краен случай да се направи така, че от прозорците и вратите да не се наблюдават екраните на мониторите и принтерите.

При голяма, централизирана система, в която много от данните са поверителни, сървърите трябва да са физически обезопасени от случайно или умишлено повреждане. Винаги се намират хора, желаещи да демонстрират своите технически способности, когато има проблеми със сървъра. Поради това най-добре е физически да се елиминира възможността случайни лица да имат достъп до сървъра. Най-простото решение е той да се заключи в отделна стая, до която

достъпът да е ограничен. Така ще се гарантира неговата сигурност.

Опасността от пожари е твърде голяма и щетите, които нанасят – също, така че противопожарната защита е съществена част от физическата защита. Не може да се измислят нови методи за борба с огъня. Необходимо е в помещенията, където се намират компютърните системи, да има противопожарна сигнализация и автоматични средства за пожарогасене.

Към поддържащата инфраструктура може да се отнесат системите за елекро-, водо- и топлоснабдяване, средствата за комуникация. Към тях трябва да има същите изисквания за достъпност и цялостност, както и към информационните системи. За осигуряването на цялостност е необходимо оборудването да се защити от кражби и повреди.

Нерегламентираният достъп до данните може да се осъществи по различни начини: наблюдаване на екрана на монитора, четене на пакети, предавани по локалната мрежа, анализ на излъчваните електромагнитни вълни и др. За съжаление, някои от способите за прехващане на данни са доста достъпни, борбата с тях е трудна и скъпа. Мобилните и преносимите компютри също са много достъпен обект за нерегламентиран достъп. Според действащото законодателство за тях се изготвят специфични изисквания за физическа сигурност. Такова може да бъде например шифроването на данни на дисковете на лаптопите.

Като цяло трябва да се отбележи, че физическата защита се базира на здравия разум, който подсказва целесъобразните решения.

Поддържане на работоспособност

През време на експлоатацията на автоматизираните информационни системи или мрежи съществуват най-големи опасности за тяхната сигурност. Неволните грешки на системния администратор и на потребителите могат да доведат до повреди на апаратурата, разрушаване на програмите и данните, в най-добрия случай се допускат слабости, които повишават рисковете от заплахи. Скъпите мерки за сигурност губят своя смисъл, ако са недобре документирани, в конфликт с други програмни продукти, а паролите на системния администратор не се сменят от момента на монтирането. Именно затова, за осигуряване на по-добра защита на информацията в автоматизираните информационни системи или мрежи, е необходима ежедневна дейност по поддръжката.

Поддръжката на потребителите например се състои в консултиране и оказване на помощ при разрешаването на различни проблеми. Важно е в потока от въпроси на потребителите да се доловят проблеми, свързани с информационната сигурност. Многото проблеми може да бъдат следствие от заразяване с вируси или действия на хакери в мрежи, които имат вход в глобалната мрежа. Практически полезно е администраторите да записват въпросите на потребителите, за да могат да извлекат най-често възникващите проблеми и да направят бележки със съвети за най-разпространените проблеми.

Поддръжката на програмното осигуряване също е важна за осигуряването на цялостност на информацията. Ако потребителите имат право сами да си инсталират програмни средства, това крие опасност от заразяване с вируси. Големи опасности крие и включването към интернет. Действащото законодателство е категорично, че автоматизираните информационни системи или мрежи, в които се създава, съхранява, обработва и пренася класифицирана информация, не може да бъдат свързани с глобални мрежи. Въпреки това трябва да се контролират самоволни действия на потребителите по програмните ресурси. Във връзка с това трябва да се осъществява контрол и за нерегламентирани промени в програмите и правата за достъп до тях.

От практиката е доказано, че колкото по-автоматизиран е един процес, толкова по-малко вероятни са грешките, така че може да се твърди, че автоматизацията е стълб на сигурността.

За възстановяването на програмите и данните след аварии абсолютно необходимо се оказва архивирането. И тук е добре процесът да бъде автоматизиран, а копията да се съхраняват на безопасно място, защитено от пожари и други заплахи.

Документална сигурност

При поддържането на работоспособността и по време на работния процес се налага да се осигурят физическа защита и отчет на дискетите, лентите, разпечатаните на хартия продукти и др. Те трябва да се защитят от нерегламентиран достъп, както и от вредни влияния на околната среда. Управлението на носителите на класифицирана информация обхваща целия им жизнен цикъл. В нормативната уредба тези въпроси са строго фиксирани. Магнитните носители на класифицирана информация се завеждат в секретното

деловодство по специален ред, а при необходимост се унищожават физически. Колкото до отпечатването на материали, съдържащи класифицирана информация, най-практично и законосъобразно е с помощта на програмни средства да се определи принтер, на който да става това.

Информационните носители в организационната единица трябва да са защитени в съответствие с критичността и чувствителността на записаната върху тях информация. Критериите за сигурност трябва да се разработят в съответствие с носителя, на който се съхранява информацията (хартия, плака за прожекционен апарат, флашпамет и т.н.), системите за тяхната обработка (персонални компютри, записващи устройства и т.н.) или в зависимост от методите за пренос на информацията (електронна поща, разговор в интернет между две или повече лица и т.н.). Информацията трябва да се защитава последователно по време на нейния жизнен цикъл от създаването до нейното унищожаване, без значение къде се намира по този път, в каква форма е, как се обработва или пренася. Информационните системи следва да предоставят на собствениците и пазителите на информация адекватни механизми за проследяване на етапите на обработка и пътя на електронните трансакции.

Документалната сигурност е неизменна част от сигурността на класифицираната информация в автоматизираните информационни системи или мрежи. Във вид на документ се оформя всичко – от политиката за сигурност до регистрите за отчитане на дискетите. Важността на този въпрос е отчетена в Закона за защита на класифицираната информация, където има отделен раздел, изцяло посветен на документалната сигурност.

Планиране на възстановителни работи

Нито една организация не е застрахована от природни бедствия, аварии и катастрофи, предизвикани от злонамерени действия или от небрежност и некомпетентност. В същото време във всяка организация има информация и функции, които тя смята за особено важни. Част от организацията по защитата на информацията е планирането на възстановителни работи, което дава възможност за подготовка с цел намаляване на загубите и съхраняване на способността за функциониране на системата, макар и в минимален обем. Процесът на планиране може да се раздели на следните етапи:

- Определяне на критически важните функции, установяване на приоритетите;
- Идентификация на ресурсите, необходими за изпълнението на критически важни функции;
- Определяне на списък на възможните аварии;
- Разработка на стратегия на възстановителни работи;
- Подготовка за реализация на изработената стратегия;
- Проверка на стратегията.

При планирането на възстановителните работи трябва да се има предвид, че пълно съхраняване на информацията невинаги е възможно. Необходимо е да се определят критично важните функции, без които организацията губи функционалността си, и да се изведат приоритетите, за да може по-бързо и с минимални загуби да се възобнови дейността след аварията.

Критичните организационни ресурси са:

- Персонал;
- Информационна структура;
- Физическа инфраструктура.

Планирането на възстановителните работи трябва да предписва не толкова дейности по временна схема, колкото мероприятия за връщане към нормално функциониране. Подготовката за това се състои в изработването на подробен план за действие в извънредни ситуации и осигуряването на резервни ресурси. Последното може да се постигне без голям разход на средства, ако се сключат споразумения с една или няколко организации за взаимна поддръжка в случай на авария. Важна част от подготовката за възстановяването е обучението на персонала.

С изложеното дотук се изчерпа прегледът на основните организационни мерки за защита на класифицираната информация в автоматизирани информационни системи или мрежи. Тези мерки се осигуряват със съответните програмно-технически средства, на които ще се спрем по-долу.

ПРОГРАМНО-ТЕХНИЧЕСКИ АСПЕКТИ НА ЗАЩИТАТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ В АИС ИЛИ МРЕЖИ

Програмно-техническите мерки са последната и най-важна част на информационната защита. Основната част от загубите се нанасят от действията на легалните потребители, по отношение на които управленските и организационните мерки не дават ефект. Главните врагове са некомпетентността и неточността на персонала при изпълнението на служебните задължения и опитите за нерегламентиран достъп до системите. Само програмно-техническите мерки са в състояние да ги неутрализират. Към програмните методи за защита се отнасят:

- Идентификация и автентикация;
- Управление на достъпа;
- Протоколиране и одит;
- Защита от вируси.

Към техническите методи за защита се отнасят:

- Криптиране на данните;
- Екраниране;
- Използване на терминали;
- Използване на непрекъсваемо електрозахранване.

В последните години се забелязва динамично развитие на програмно-техническите мерки за защита. Тяхното обновяване се стимулира от също толкова бързото развитие на мерките за техническо разузнаване, включително с използването на програмни средства.

ПРОГРАМНИ СРЕДСТВА ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Идентификация и автентикация

Идентификацията и автентикацията формират първата линия на защита на информационното пространство на организационната единица. Без ред на входа няма ред и на охраняваната територия. Идентификацията позволява на субекта да назове себе си (да съобщи името си). Посредством автентикацията втората страна се убеждава, че субектът е действително онзи, за когото се представя.

В качеството на синоним на термина „автентикация“ понякога се използва терминът „проверка на идентичността“. Субектът може да потвърди своята идентичност, като демонстрира едно от следващите качества:

- Нещо, което той знае (парола, личен идентификационен номер, криптографски ключ и пр.);
- Нещо, което той притежава (електронна лична карта или друго устройство с аналогично предназначение);
- Нещо, което е уникална част от самия него (глас, отпечатъци от пръсти, роговица на окото и т.под.).

Надеждната идентификация и автентикация са затруднени по редица причини. Първо, компютърната система използва информация във вид, в който е била получена. Второ, почти всички автентикационни същности може да се узнаят, откраднат или подправят. Трето, има противоречие между надеждната автентикация и удобството на потребителя. И четвърто, колкото по-надеждно е едно средство за защита, толкова е по-скъпо.

Най-често разпространеното средство за автентикация са паролите. Системата сравнява въведените и по-рано зададени от потребителя пароли и в случай на съвпадение идентичността на потребителя се смята за доказана. Друго средство, което постепенно набира популярност, са секретните криптографски ключове. Главните достойнства на паролната автентикация са простотата и удобството. При правилно използване паролите могат да осигурят приемливо за много организации ниво на защита. Надеждността на паролата се основава на възможността да се запомни и пази в тайна. За да се запомня лесно, паролата често се прави елементарна (името на близък, название на коли, отбори и т.н.), което е грешно, защото не е трудно да се отгатне. Паролите може да бъдат разбрани по много начини: може да бъдат видени чрез използване на специални прибори, често се съобщават на колеги, може да бъдат разшифровани с програмни средства или да бъдат прехванати по електронен път.

На практика единственият изход е използването на криптографията за шифроване на паролите. Препоръчват се следните мерки за повишаване на надеждността:

- Налагане на технически ограничения – паролите да не са кратки, да съдържат букви, цифри и други знаци;

• Управление на сроковете за действие на паролите, тяхната периодична смяна;

• Ограничаване на достъпа до файла с паролите;

• Ограничаване на броя на несполучливите опити за вход в системата;

• Обучение на потребителите;

• Използване на програмни генератори на пароли.

Както е известно, едно от най-мощните средства в ръцете на злонамерени лица е изменението на програмата за автентикация, при което паролата не само се проверява, но и се запомня за последващ нерегламентиран достъп.

Устройствата за контрол, базирани на биометрични характеристики, са скъпи и сложни, затова се използват само в специфични организации с високи изисквания за сигурност. Администрирането на идентификацията и автентикацията е много важна и трудна задача. Необходимо е постоянно да се поддържат конфиденциалност, цялостност и достъпност. Най-лесният начин това да става, е като се централизира процесът на администриране, което позволява да се реализира концепцията за единен вход. След като премине проверката за идентичност, на потребителя му се дава достъп до всички ресурси на мрежата (в пределите на неговите правомощия).

За да се въведе ефективна система за защита, се препоръчва следната автентикационна политика:

1. Потребителски идентификатори и пароли. За да се реализира принципът за *необходимо знание*, организационната единица трябва да изисква всеки служител, имащ достъп до нейните автоматизирани информационни системи или мрежи, да има уникален потребителски идентификатор и лична парола. Този потребителски идентификатор след това се използва за ограничаване на системните права, като се отчитат служебните задължения и отговорности. Всеки служител е персонално отговорен за използването и опазването на своя потребителски идентификатор и лична парола.

2. Анонимен потребителски идентификатор. Забранява се анонимното влизане в АИС или мрежи на организационната единица. Изключение правят публичните електронни форуми за съобщения, сайтовете в интернет, интранет и други системи, които са проектирани по такъв начин, че ползват анонимен потребителс-

ки идентификатор за нормална работа. Потребителят винаги трябва да използва потребителски идентификатор, за да се легитимира пред АИС или мрежи на организационната единица и да е ясно какви действия извършва.

3. Трудни за отгатване пароли. Паролите, които потребителите избират, трябва да са трудни за отгатване с цел да не се компрометира цялостната работа на информационните системи. Паролите не трябва да са свързани нито с работата, нито с личния живот. Например регистрационен номер на лек автомобил, имена на близки и роднини, части от адреси, имена, запазени марки и др. Паролата не трябва да е дума, която може да се открие в речник. Да не се използват технически термини, жаргон и др.

4. Лесно запомнящи се пароли. Потребителите трябва да избират лесни за запомняне пароли, които в същото време са трудни за отгатване. Например:

- Слепване на няколко думи заедно;
- Изместване на думата или част от нея при набиране от клавиатурата – ред нагоре, вляво, вдясно или надолу;
- Използване на горен и долен регистър за различни символи в паролата;
- Трансформиране на стандартна дума в съответствие с някакво правило;
- Комбиниране на букви, цифри и пунктуационни символи в паролата;
- Създаване на акроним от известна поредица от думи, като песен, стихотворение и др.;
- Грешно изписване на дума;
- Комбиниране на няколко неща по начин, който ви харесва, като желание, любими неща – цвят, храна, място за почивка и др.

5. Повторение на шаблони при паролите. Потребителите не трябва да конструират паролите чрез базова поредица от символи, която след това частично се променя според някакво предсказуемо правило. Потребителят трябва да избира новите пароли така, че да не са подобни на преди това ползвани пароли.

6. Задължителни изисквания за паролите. За да се отгатнат потрудно паролите, е необходимо те да са с най-малко 6 символа дължина. За да е сигурно, че компрометираните пароли няма да се използват продължително време, паролите трябва да се сменят на

всеки 60 дни или по често. Ако има подозрение, че една парола е известна на друго лице или група лица, тя трябва незабавно да се смени.

7. Съхранение на паролите. Паролите да не се съхраняват в явен вид във файлове за пакетна обработка, скриптове за автоматизирано влизане в системите, макроси, функционални клавиши на терминали, в компютри, които нямат система за контрол на достъпа, или на други места, където неупълномощени лица могат да ги открият. Също така паролите не трябва да се записват под каквато и да е лесна за разчитане форма и да се оставят на леснодостъпни места.

8. Съвместно използване на пароли. Съвместното използване на пароли и/или потребителски идентификатори е забранено. Допустимо е изключение от това правило в случаите, когато естеството на информационната система го налага и само след специално разрешение от страна на *Собственика* на информацията.

9. Съглашение. Всички служители на организационната единица трябва да подпишат декларация, преди да използват своя потребителски идентификатор. Ако потребителят вече има потребителски идентификатор, документът трябва да се подпише преди получаването на нов потребителски идентификатор. Подписването на това съглашение показва, че потребителят разбира и приема политиките и процедурите на организационната единица, свързана с използването на компютрите и мрежите. Декларациите се съхраняват в личното кадрово дело на всеки служител на организационната единица.

Управление на достъпа

Средствата за управление на достъпа позволяват да се характеризират и контролират действия, които субектите (потребители и процеси) могат да изпълняват над обектите (информации и други ресурси). Тук става дума за логическо управление на достъпа, което се реализира с програмни средства. Ако има съвкупност от субекти и обекти, задачата за логическо управление на достъпа се състои в определяне на списък от допустими операции за всеки субект и обект, като съответствието им се контролира по предварително установен ред.

Контролът на правата на достъп се създава от различни компоненти на програмната среда: операционната система, допълнителни средства за сигурност, управление на база данни, посредническо-

програмно осигуряване и т.н. При вземане на решение за предоставяне на достъп обикновено се анализира следната информация:

- Идентификатор на субекта – идентификатор на потребителя, мрежов адрес на компютър и т.н.;
- Атрибути на субекта – белегът за сигурност, групата на потребителя;
- Място на действие;
- Време на действие;
- Вътрешни ограничения на програмата.

Мнозинството операционни системи и системите за управление на бази данни реализират произволно управление на достъпа. Основното му достойнство е гъвкавост. Всеки субект може независимо да задава права за достъп, което е особено лесно, ако се използва списък за управление на достъп. Този подход има редица недостатъци. Децентрализацията на управлението на достъпа води до това, че надеждни трябва да бъдат много потребители, а не само системните оператори и администратори. Разсеяността и некомпетентността на притежателя на секретна информация може да доведе до откриването ѝ на всички потребители.

В заключение трябва да се подчертае важността на управлението на достъпа, което трябва да бъде заложено в съществуващата политика за сигурност. Тя трябва да бъде обект на квалифицирано системно администриране.

Протоколиране и одит

Под „протоколиране“ се разбира събиране на информация за събития, които се случват в информационната система. Реализацията на всеки програмен продукт е набор от възможни събития. Те може да се подразделят на вътрешни (предизвикани от действията на самия продукт), външни (предизвикани от действия на други продукти) и клиентски (предизвикани от действията на потребителите и администраторите).

Одитът е анализ на събраната информация, провеждан оперативно, в реално време или периодично. Целите на протоколирането и одита са:

- Осигуряване на отчетността на потребителите и администраторите;
- Възможност за реконструкция на последователността на събитията;

• Регистриране на опитите за нарушаване на информационната сигурност;

• Предоставяне на информация за проявленията и анализа на проблемите.

Протоколирането трябва да се ръководи от здрав разум. На тази основа се решава какви събития да се регистрират и с каква степен на детайлизация. Необходимо е да се обърне внимание на достигането на целите, от една страна, а от друга, разходите за ресурси да не напускат разумните граници. Твърде детайлното протоколиране не само снижава производителността, но и затруднява одита.

Друга особеност на протоколирането и одита е зависимостта от други средства за сигурност. Идентификацията и автентикацията служат като отправна точка за отчетността за потребителите. Осигуряването на отчетност е важно като средство за предупреждение. Ако потребителите знаят, че техните действия са фиксирани, те ще се въздържат от незаконни операции. Очевидно е, че ако даден потребител се подозира в опити за нерегламентиран достъп, неговите действия може да се регистрират особено детайлно, като се стига до всяко натискане на клавиш. Това само по себе си защитава целостността на информацията.

Реконструкцията на последователността на събитията позволява да се открият слабостите на защитата на системата, да се намери виновникът, да се оцени мащабът на причинената вреда и системата да се върне към нормална работа. Анализът на проблемите може да помогне да се подобри такъв параметър на защитата, като достъпност.

Прекаляването с протоколирането и одита може да ги превърне в безсмислена формалност, но въведени с мярка, те могат да бъдат ефективен инструмент за поддържане на информационната сигурност.

Защита от компютърни вируси

Когато се разработват процедурите за защита на една мрежа, трябва да бъде взета предвид и опасността от разпространяването на вируси. За защита от вируси се използват специални антивирусни програми. По принцип е невъзможно да бъде създадена програма, защитаваща от всички възможни вируси. Антивирусните програми:

• предотвратяват активирането на вирусите;

• премахват вирусите;

- възстановяват причинени от вируси щети;
- държат вирусите под контрол след тяхното активиране.

Един от най-добрите начини за предпазване от вируси е предотвратяването на нерегламентиран достъп. За целта администраторът трябва да вземе всички предпазни мерки. Политиката за въвеждане на антивирусна защита на клиентските компютри и мрежовите сървъри е част от политиката за сигурност на АИС или мрежи.

ТЕХНИЧЕСКИ СПОСОБИ ЗА ЗАЩИТА

Криптография

Едно от най-мощните средства за защита на конфиденциалността и целостността на информацията е криптографията. В много отношения тя заема централно място сред програмно-техническите регулатори на сигурността, представлявайки основна реализация, а понякога и единствен начин за защита. Например при преносимите компютри, където физическата защита е много трудна, само криптографията позволява да се гарантира конфиденциалността на информацията, даже в случай на кражба. Има два начина за криптиране на данните – софтуерен и хардуерен.

При софтуерния начин криптирането на данните се извършва със специална помощна програма. Данните, изпратени по мрежата, са „разбъркани“ по някакъв алгоритъм. Така, дори някой да се закачи към кабела и да открадне данни, тяхното разчитане е изключително сложно и практически трудно осъществимо. Когато данните стигнат до получателя, помощна програма декодира криптираните данни и отново ги превръща в разбираема информация. Модерните методи за криптиране автоматизират и двата процеса – криптиране и декриптиране.

При хардуерните системи за криптиране се използва специална електронна апаратура.

Много важна част от една компютърна мрежа са кабелите. Всеки кабел действа като антена и излъчва в ефира сигнал, макар и с много малко ниво. Това обаче е напълно достатъчно сигналът да бъде уловен с подходящо електронно устройство за подслушване. Информацията може да бъде откраднатa и директно от самия кабел с помощта на съответно оборудване. Затова до кабелите, по които се предава поверителна информация, достъп трябва да имат

само оторизирани лица. Това може да се осъществи при подходящо планиране, като кабелите се прокарат по добре защитени трасета.

За подобряване на сигурността на компютърната мрежа е много важно също какви кабели ще се използват. Относително най-сигурни са кабелите с оптични нишки. При кабела с оптични нишки информацията се пренася под формата на модулирани светлинни импулси. Това е относително безопасен начин за пренасяне на данни, тъй като по кабела не се пренасят електрически импулси, които може да бъдат регистрирани, за да се откраднат данни. Последното е възможно при всички видове медни кабели.

Екраниране

В известен смисъл всеки ресурс се пази от защитна стена. В тази стена има „врати", през които потребителите могат да преминат, за да достъпят ресурса. Някои врати позволяват на потребителя да прави повече неща с ресурса, отколкото други. Администраторът определя кои потребители през кои врати могат да минават. Някои врати позволяват пълен достъп или пълен контрол над ресурса, докато други предоставят достъп например само за четене. Всеки поделен ресурс или файл съдържа списък с потребителите или групите и асоциираните с тях позволения (врати).

Използване на терминали

Терминалите, или бездисковите компютри, нямат флопи и хард дискове. Те могат да правят всичко по същия начин, както компютрите с дискове, освен че не могат да записват данни върху дискета или локален твърд диск. От гледна точка на сигурността тези компютри са подходящи, защото потребителят не може да свали файлове и да ги вземе със себе си. Бездисковите компютри не се нуждаят от диск за първоначално зареждане. Те могат да комуникират със сървъра и да влизат в системата благодарение на специален чип за първоначално зареждане, инсталиран на мрежовата адаптерна карта. При включването на бездисков компютър чипът изпраща съобщение на сървъра, че желае да зареди. Сървърът отговаря, сваляйки зареждащ софтуер в RAM паметта на бездисковия компютър, и автоматично показва на екрана прозореца за влизане в системата като част от процеса на зареждане. След като потребителят влезе, компютърът е свързан към мрежата.

Използване на непрекъсваемо електрозахранване

В случай на бедствие, предизвикано от проблеми в електрозахранването, необходимото време за възстановяване на данните от архива може да доведе до сериозно намаляване на продуктивността. Има начин за подсигуряване срещу загуба на данни чрез използване на непрекъсваемо електрозахранване (UPS).

UPS е автоматизирано външно захранващо устройство, което поддържа работата на сървъра и на други устройства дори когато спре електрозахранването. То се разполага между сървъра и източника на електрозахранване. Стандартните UPS устройства осигуряват два критично важни компонента за мрежата:

- източник за захранване на сървъра за определено време;
- безопасно изключване на системата.

При прекъсване на електрозахранването UPS системата предупреждава потребителите да прекратят работата по текущите задачи. След това изчаква предварително зададен период от време и изключва системата.

Разгледаните дотук мерки за защита масово се прилагат на практика, но в хода на работата в организационните единици възникват множество въпроси, отговорите на които зависят от конкретните приложения. От чисто практическа гледна точка може да бъдат направени конкретни предложения, които ще улеснят работата на органите по сигурността, администраторите и потребителите:

1. Ръководителите на организационните единици трябва да осигурят добра координация между отделите „Човешки ресурси“ и администраторите на мрежата. Така същите ще бъдат уведомявани своевременно за новоназначени, преместени и напуснали служители, за даване и респективно отнемане на права за достъп до класифицирана информация в съответните организации;

2. Администраторите на мрежата трябва да следят за новостите в организационно и техническо отношение за защита на класифицираната информация и да информират за тях ръководството и потребителите. Последните освен обучение във връзка с прилагането на Закона за защита на класифицираната информация и подзаконовите актове биха могли да преминат и обучение по отношение на защитата на сигурността на персоналните си компютри и данните, които създават, обработват и съхраняват на тях;

3. В организационната единица трябва да бъде заведено Ръководс-

тво на потребителя, където: (а) да бъдат описани най-честите проблеми при работата с програмните продукти в съответната организационна единица; (б) да бъдат посочени решения на тези проблеми; (в) да бъдат описани подходящи методи за защита на персоналната информация на всеки потребител с достъп до класифицирана информация.

Даденото дотук описание на политиката за защита на класифицираната информация в компютърните системи за управление при бедствия, аварии и катастрофи не може да има претенциите за абсолютна цялостност и завършеност. То отразява основни положения в организацията и изпълнението на тези мерки, произтичащи от действащата у нас регулаторна рамка. Тъй като в бъдеще все повече ще се налага да се навлиза в тези проблеми, настоящата работа може да послужи за основа за разработка на конкретни специфични изисквания за защита на класифицираната информация в автоматизираните информационни системи или мрежи.

МЕТОДИ ЗА ОЦЕНКА НА ПОЛЗИТЕ И РАЗХОДИТЕ ОТ ИНВЕСТИРАНЕ В ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ В АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ ИЛИ МРЕЖИ

Разходи за защита на класифицираната информация в автоматизираните информационни системи или мрежи

Въпреки че разходите за защита на класифицираната информация се определят по-лесно, отколкото ползите от тях, те също могат да предизвикат някои проблеми. Обикновено се допуска грешката да се пропускат разходи и по тази причина проектът да изглежда по-печеливш, отколкото е в действителност. Представеният по-долу списък е съставен, за да се избегнат подобни пропуски:

- Хардуер. Не само самите компютри, но и всички останали технически съоръжения, включително окабеляването, принтерите и т.н., трябва да се отчитат;
- Софтуер. Дори когато софтуерът е за широка употреба, е много вероятно да има допълнителни разходи по настройването му за работа;

• Инсталация. Включва разходите за конвертиране на данните от действащата система, паралелна употреба, мониторинг и др.;

• Работна среда. Това се отнася до непосредствената заобикаляща среда, например мебелировка и вентилация;

• Текущи. Например разходи за електричество, за телефон и т.н.;

• Поддръжка. За аварии и ремонти;

• Създаване на вградена компютърна мрежа. Например за планиране, координация, управление и контрол на защитата, със съответната инфраструктура;

• Обучение. Основно – за потребителите;

• Допълнителни организационни разходи. Основно – в отделите, засегнати от система за защита на класифицираната информация. Например увеличено време за контрол и диспечиране на потребителите.

След като ползите и разходите се определят правилно, може да започне оценяването на инвестициите в системата за защита на класифицираната информация в автоматизираната информационна система или мрежа и да се направи предложение за дългосрочен план за нейното изграждане.

Какво изискват системните организационни единици от един метод за оценяване на инвестициите в система за защита на класифицираната информация в автоматизирана информационна система или мрежи?

Организациите могат да искат да оценяват проекта за изграждане на система за защита на класифицираната информация на всяко от нивата на неговото развитие и внедряване. Основните нива тук са:

1. Концепцията е развита. Тя трябва да се развива едновременно с бизнес стратегията и ролята ѝ трябва да бъде оценена при общи условия. Резултатът може да бъде съвкупност от проекти, някои от които са обвързани със специфични инициативи, а други – с изискванията на инфраструктурата;

2. Определен е точен проект. Това може да бъде искане или решение за инсталиране на система за защита на класифицираната информация със съпътстващата инфраструктура. На този етап обикновено разходите по проекта трябва да бъдат оправдани в контекста на другите капитални инвестиции и да се направи избор

на най-подходящия дизайн, който да покрива всички изисквания, определени в спецификацията;

3. Проектът е в етап на развитие. Трябва да се правят проверки, за да бъде сигурно, че вътрешните и външните промени не са повлияли на приложимостта на проекта. В същото време напредъкът трябва да бъде оценен, за да е сигурно, че се движи в рамките на бюджета си;

4. Проектът е готов за подпис. Отговорността е прехвърлена към ръководителя на организационната единица. Той трябва да положи своя подпис, за да удостовери, че системата за защита на класифицираната информация ще извършва в автоматизираната информационна система или мрежа това, което се изисква от нея;

5. Проектът току-що е бил внедрен. Системата е проверена, за да е сигурно, че работи, както е планирано, и вече носи очакваните ползи;

6. Проектът функционира от известно време. Оценяването на този етап следи влиянието на проекта, сравнявайки действителните разходи и ползи с планираните такива, определя неочакваните ползи и разходи и съхранява научените уроци за в бъдеще;

7. Проектът наближава своя край. Разглеждат се варианти за неговата смяна.

Изследванията на начина на поведение на голям брой организационни единици показва, че те не са съвсем наясно с различните цели на оценяването на инвестициите в системата за защита на класифицираната информация в автоматизираните информационни системи или мрежи и може да объркат неговите етапи.

Методи за оценка на ползите и разходите от инвестиране в система за защита на класифицираната информация в АИС или мрежи

От съществуващата литература е видно, че има множество възможни методи и подходи за оценяване, всеки от които притежава специфични характеристики и целенасоченост. По-надолу ще посочим някои от тези методи, започвайки с някои от най-типичните и широко разпространени.

Оценка на възвръщаемост на инвестициите (ОВИ)[10]

Този подход включва множество съществени инвестиционно оценителни подходи. Може би най-известните от тях са тези, които, базирайки се на предположението, че бъдещите ползи са обект на някои намаляващи себестойността фактори, оценяват текущата стойност на бъдещите парични потоци. ОВИ подходите обикновено се използват от организации със строга финансова дисциплина. Основната сила на методите от тази категория е, че те позволяват на вземащите решение да сравнят приблизително определените бъдещи приходи от различни инвестиции. Недостатък е, че някои добри инвестиционни възможности се пренебрегват, защото е трудно ползите от тях да се оценят като приходи. Най-широко използваният такъв подход е анализът „приход – разход", произлизащ от класическото счетоводство. Този метод се прилага, когато ползите може да бъдат изцяло отдадени на промяната в системата и се приемат под формата на спестяване на разходите. Разновидност на този метод е методът SESAME, предложен от IBM[11]. При него се изчислява каква би била цената на дадена функционалност, ако тя се реализира без използването на система за защита на класифицираната информация.

Анализ на ползите от разхода (АПР)[12]

Този подход се опитва да намери (изчисли) стойността на парите за всеки елемент от разходите и ползите от експлоатацията на проекта. Методът се е появил вследствие на опита да се реши проблемът, че някои елементи, приемани за ползи или за разходи, нямат ясна пазарна стойност или цена, докато други елементи, водещи до извършване на разход или постигане на ползи, са външни за компанията инвеститор. Всички ползи и разходи се определят като парична стойност на базата на някаква теория за оценяване. Получените стойности на ползите и разходите може да бъдат включени

---

[10] ROI – Return of Investment.

[11] **Lincoln**, T. Retrospective appraisal of IT using SESAME. – In: **Information** Systems Assessment: Issues and Challenges, edited by N. Bjorn Andersen and G. Davis. North Holland, Amsterdam, 1998.

[12] CBA – Cost Benefit Analysis.

в модел за вземане на решения, базиран на някои от стандартните ОВИ методи. Основният недостатък на този класически метод е изкуственото естество на някои от използваните метрики – заместители.

Информационна икономика[13]

Това е разновидност на анализа на отношението „приходи – разходи", разработена специално за оценяване на проекти за внедряване на система за защита на класифицираната информация в автоматизираните информационни системи. Целта на този метод е да идентифицира и измери икономическото влияние на промените, настъпили вследствие на въвеждането на нова защита в организацията. Той се занимава със системи, които носят ползи чрез подобряване на защитата на връзките и комуникациите между различните отдели в организацията. Засяга иновациите и оценяването на инвестициите, когато финансовите въпроси се променят от измерване към оценяване и избиране измежду нови, неизпитани и недоказани алтернативи. Методът разглежда стратегическата и технологичната несигурност и организационния риск като разходни елементи, които трябва да бъдат оценявани.

Многообектни и многокритериални методи (МММ)[14]

Според този метод стойността на проекта може да бъде измервана не само в пари. МММ позволява на вземащите решения да оценят относителната стойност на различни перспективи в условия, каквито те предпочитат. Резултатът е, че проектът се оценява по практическата си приложимост, а не по паричната си стойност. МММ е добре приложим, когато има голям брой възможни обекти за защита в много различни структурни звена в организационната единица. Той има голяма стойност на етапа, в който се определя политиката. Подходящ е също когато има няколко алтернативи и е трудно да се избере между тях, защото не всички те предлагат еднакъв изход.

---

[13] **Parker**, M. M., R. J. **Benson**, H. E. **Trainor**. Information Economics. Prentice Hall International, 1988.

[14] **Land**, F. Multi-objective, multi-criteria (MOMC) methods – Evaluation of System's Goals in determining a decision strategy for computer-based information systems. – In: *Computer Journal*, 19 (4), 1976.

Ограничаващи величини[15]

Предлага груба оценка на похарченото за системата за защита на класифицираната информация. Базира се на съотношението между сумарните разходи и останалите агрегатни стойности.

Възвръщаемост на мениджмънта[16]

Този метод представлява стойността, отдавана на система за защита на класифицираната информация като вътрешна промяна към вече съществуващо ниво на управление на сигурността.

Анализ на стойността[17]

Този метод се опитва да оцени широк спектър от ползи, включително трудно доловимите. Методът се основава на идеята, че е много по-важно да се концентрираме върху стойността (добавената), отколкото върху спестения разход.

Експериментални методи

Те са се появили сравнително скоро в контекста на оценяването на проекти. Доскоро можеше да се оценява само точното влияние на въвеждането на нови системи за защита на класифицираната информация в автоматизираните информационни системи, защото инвестицията в развитието на такива системи до етапа, в който се получава действителният ефект от тях, беше много голяма. Днес многообразието от софтуерни инструменти и симулационни методи дава възможност за по-бързо и по-евтино разработване на прототипи или модели на нови системи.

Има три основни категории експериментални методи:

1. *Създаване на прототипи*[18] (Prototyping) – свързано е с бързото разработване на прототипи от системата за защита на класифицираната информация, обикновено с използване на програмен

---

[15] **Martin**, R. Boundary Values – "Utilization and Efficiency". Working Paper RDP/90/4, Oxford Institute of Management, 26.

[16] ROM – Return of Management.

[17] **Rivard**, E., K. **Kaiser**. Value Analysis – "The Benefits of Quality IS". Datamation, January 1989.

[18] **Alavi**, M. An Assessment of the prototyping approach to IS development. Communications of the ACM, 27, 1984.

език от четвърто поколение. Прототипът се тества и се оценява, и при необходимост се преработва и се тества отново;

2. *Симулация* (Simulation) – това вероятно е методът с най-дълга история. Той включва изграждането на модел на предлаганата система за защита на класифицираната информация и използването на този модел като основа, върху която да се провеждат експерименти;

3. *Изпълнение на симулационни игри* (Game playing)[19] – може да се използва за оценяване на резултата от промяната в начина на защита на класифицираната информация и решаване на определени задачи.

В специализираната литература също са описани голям брой методи, които може да бъдат наречени комбинирани.[20] Те съчетават различни аспекти от повечето методи, описани по-горе. На практика много организации комбинират части от различните методи и ги променят според ситуацията.

Фактори, влияещи върху оценяването

Оценяването на ефективността от внедряването на система за защита на класифицираната информация е необходимо да се извършва на различните нива от развитието на всеки проект за внедряване на автоматизирана информационна система. Преди внедряването организациите трябва да вземат решение дали има смисъл да инвестират в него. Какво предлага той в сравнение с други такива ИС проекти? Дали приходите от него ще превишат предварително определените от организацията? След като се внедри проектът, организациите вече искат да знаят дали той е бил сполучлив. Дали е донесъл обещаните ползи. Дали повишените разходи за защита на класифицираната информация са оправдани.

Целта и намирането на подходящия момент за оценяване са два от факторите, които могат да влияят върху извършването му. Както вече споменахме, търсенето на един-единствен метод, който

[19] **Etzerodt**, P., K. H. **Madsen**. IS assessment as a learning process. – In: **Information** Systems Assessment: Issues and Challenges, edited by N. Bjorn Andersen and G. Davis. North Holland, Amsterdam, 1989.

[20] **Earl**, M. Management Strategies for Information Management. Prentice Hall, 1989.

да може да се справи с оценяването на инвестициите за система за защита на класифицираната информация в автоматизирани информационни системи или мрежи се оказа безплодно. Това е така, защото спектърът от условия, към които този метод трябва да бъде приложен, е толкова широк, че нито един от изброените методи не може да се справи.

Всеки проект за изграждане на автоматизирана информационна система има характеристики, които влияят върху избора на подходящ метод за оценяване на нейната защита. Затова спектърът от условия е толкова широк. В същото време всеки такъв метод има характеристики, които се отнасят само за определени условия, при които той може да се приложи. Ето защо първата стъпка в оценяването е да разберем повече за контекста, в който ще се извърши то.

Факторите, които влияят върху начина, по който се вземат решенията за инвестиране в система за защита на класифицираната информация, може да се класифицират в пет основни групи:

- Роля на оценяването;
- Среда, в която е прието да се извърши оценяването;
- Характеристики на системата;
- Характеристики на организацията;
- Спецификата, която свързва причини и резултат, т.е. инвестицията и ползите от нея.

Роля на оценяването

Ролята на оценяването се определя от момента и нивото, на което се провежда.

Първо, моментът от проекта за изграждане на система за защита на класифицираната информация, в който се извършва оценяването, има отношение към използвания за целта метод. Ясно е, че на всяко ниво от развитието му възникват различни въпроси. В началните нива основна грижа са схематичното дефиниране на най-важните цели и скицирането на трудностите. Методът на ограничаващите величини не е много задълбочен, не изисква подробни изчисления и приблизително показва сравнителното положение на проекта. Ето защо се смята, че този метод е подходящ за ситуацията. Поради различни причини методите МММ също се смятат за подходящи в началните етапи за постигането на консенсус на високите нива.

Докато в ранните етапи основна грижа на управлението е опре-

делянето на обхвата на политиката, за което спомагат методите за оценка, на следващо ниво вече се изискват по-точни спецификации за това какво трябва да постигне проектът. Тогава проблемът е по-скоро в измерването и определянето на точното влияние на системата за защита на класифицираната информация, като едновременно се отчитат разходите, които ще бъдат извършени, и ползите, които се очаква да се получат вследствие на нейната употреба.

Среда, в която се извършва оценяването

Средата, в която трябва да се вземе решение, може да бъде повече или по-малко ограничена. Оценяването може или да отговаря на съществуващите организационни похвати, или да не почива на установена практика. Вземащите решения лица могат да разглеждат само точно изчислимите величини или да са доволни, ако имат яснота по качествените ползи. Разходът за оценителната процедура може също така да се вземе предвид, както и способността на персонала, обучен за употребата на метода.

Система, стояща в основата на инвестициите при защита на класифицираната информация

Тази система може да бъде описана с помощта на две променливи. Първата променлива е естеството на системата – дали тя представлява някакво локално приложение, или подсигурява дадена инфраструктура.

Втората променлива е връзката между системата и естеството на работа на организацията – дали системата има епизодична поддържаща роля, или е в основата на целия работен процес.

Критерият, по който трябва да бъде оценена системата, следва да отразява естеството и предназначението ѝ. Поради тази причина методът за оценяване трябва да включва или да осигурява средства за формирането на тези критерии.

Организацията, извършваща инвестицията

Конкурентоспособната позиция на организацията също може да повлияе на оценяването. Фактор за това е мястото ѝ в бранша – дали е в стабилна позиция, дали търпи или се прогнозира в бъдеще да търпи много промени – преструктуриране и високи нива на развитие. Стабилната позиция предполага, че организацията разполага със сигурни данни, и насочва вниманието към метод, който об-

работва детайлизирана информация – подходящ метод в случая е ОВИ. Нестабилната позиция предполага, че организацията не разполага със сигурни данни, поради което е подходящо да се използва изследователски метод – например симулация.

Вторият фактор е ръководната роля на организацията – дали се стреми да бъде новатор, или последовател. В първия случай трябва да се използват изследователски методи на оценяване, които да дават бързи резултати. Във втория случай инвестициите, направени по-рано от други организации, служат като ориентир на вземащите решение. Методът на ограничаващите величини може да се използва, за да се определят подходящите нива на разходи.

Връзка между причината и резултата

Степента, до която е възможно да се предскаже влиянието на новите системи за защита на класифицираната информация, е важен фактор при определянето на това как да се осъществи оценяването. Влиянието на новите системи може да бъде непосредствено – въвеждането на системата може да осигури по-висока конкурентоспособност и информационно превъзходство.

Но една система, конструирана така, че да осигурява на мениджъра по-добра информация с цел подобряване на процеса на вземане на решения, зависи от уменията му да използва тази информация за постигане на очакваните ползи. В случая влиянието не е пряко и за измерването му е подходящ методът МММ.

ПРОЦЕДУРИ ЗА СИГУРНОСТ НА АИС ИЛИ МРЕЖИ

Общи положения

Процедурите за сигурност са подробно описание на реда и отговорностите за изпълнение на дейностите при прилагането на утвърдените мерки за сигурност на АИС или мрежата.

Процедури за сигурност

Процедурите за сигурност се отнасят за: организацията на сигурността; физическата сигурност; персоналната сигурност; документалната сигурност; компютърната сигурност; комуникацион-

ната сигурност; сигурността при осигуряването със средства за АИС или мрежата; действията при критични по отношение на сигурността ситуации; управлението на конфигурацията; отговорностите и задълженията на потребителите.

Физическа сигурност

Зоните, в които са разположени ресурсите на АИС или мрежата, където се създава, обработва, съхранява или пренася класифицирана информация или в които е възможен достъп до такава информация, се определят като зони за сигурност. Тези зони се защитават със съответни на най-високото ниво на класификация на информацията мерки, способи и средства за физическа сигурност с цел недопускане на нерегламентиран достъп. В рамките на зоните за сигурност се определят места за:

- компютърно и комуникационно оборудване;
- въвеждане и извеждане на документи във и от системата;
- център за управление на АИС или мрежата;
- работа с криптографски средства и ключове;
- библиотеки за компютърни носители на класифицирана информация и др.

За критичните от гледна точка на сигурността места се вземат допълнителни мерки за защита, като:

- контрол на достъпа, включително с технически средства;
- системи за наблюдение;
- недопускане на присъствието само на един служител в тях.

За условия на експлоатация на АИС или мрежа, които не са свързани с конкретна глобална среда за сигурност (например мобилни, полеви и други условия), се изготвят специфични изисквания за физическа сигурност.

Персонална сигурност

Потребителите на АИС или мрежата трябва да имат разрешение за достъп до най-високото ниво на класификация за сигурност на информацията, с която имат право да работят в АИС или мрежата. Системният персонал на АИС или мрежата, както и лицата, участващи в проектирането и изграждането на системата за сигурност на АИС или мрежата, трябва да имат разрешение за достъп до най-високото ниво на класификация на информацията в АИС или мрежата.

Те преминават обучение по сигурността на АИС или мрежата, което се организира и провежда от ОРЕ за различните категории служители (системни администратори, администратори по сигурността, развойни звена, технически и обслужващ персонал). При успешно завършило обучение лицата се допускат до работа в АИС или мрежата.

Правомощията на персонала, работещ в АИС или мрежа, се определят така, че да не се допуска възможността едно лице да познава или контролира изцяло важните елементи от сигурността на АИС или мрежата.

Документална сигурност

Всички документи, съдържащи класифицирана информация, които се създават, обработват, съхраняват и/или пренасят в АИС или мрежи, се идентифицират, маркират и контролират по подходящи начини. Маркировката на документите трябва винаги да осигурява еднозначна информация за нивото на класификация при работа с тях. Начините за идентифициране, маркиране и контролиране се определят в документите по сигурността на АИС или мрежата.

Маркиране и отчет на класифицирана информация в АИС или мрежи

Класифицирана информация, създавана, обработвана, съхранявана и обменяна в сертифицирани АИС или мрежи, се маркира със съответно ниво на класификация за сигурност.

При изход на документи, съдържащи класифицирана информация, от сертифицирани АИС или мрежи:

- отпечатаните документи трябва да имат поставен гриф за сигурност и да се заведат в регистратурата;
- запис на документи се извършва само върху заведени на отчет носители в регистратурата и имащи съответно или по-високо ниво на класификация.

Регистриране, маркиране, отчет и унищожаване на материални носители за многократен запис на класифицирана информация

Материалните носители за многократен запис на класифицирана информация се водят на отчет в отделен регистър и се маркират с гриф за сигурност. Регистрационният номер и грифът за си-

гурност се поставят преди първоначалното използване на носителите за многократен запис. Върху тези носители се забранява запис на класифицирана информация с ниво на класификация, по-високо от обозначеното върху носителя.

Нивото на класификация на носител със записана класифицирана информация може да бъде понижено само след специално изтриване на класифицираната информация с ниво на класификация, по-високо от новото ниво на класификация на носителя. Специално изтриване на информация е такова изтриване, при което е невъзможно или е много трудно получаването на остатъчна информация, което налага използването на специални лабораторни методи и средства.

Нивото на класификация на носител със записана класифицирана информация може да бъде премахнато само след специално изтриване на цялата класифицирана информация, записана върху него. Специално изтриване на информацията се извършва само след като е осигурено копие на класифицираната информация, ако тя е оригинал и не се съхранява на друго място в организационната единица или на друг носител.

Забранява се понижаването или премахването на нивото на класификация на носител със записана класифицирана информация с ниво на класификация „Строго секретно".

Унищожаването на носители със записана класифицирана информация поради изтичане на експлоатационния срок на годност или по други причини се извършва:

- след като е осигурено копие на класифицираната информация, ако тя е оригинал и не се съхранява на друго място в организационната единица или на друг носител;
- след специално изтриване на класифицираната информация върху носителя;
- по начин, непозволяващ използването на носителя или на части от него и извличането на остатъчна информация.

В случай че причината за унищожаването е физическа повреда на носителя за многократен запис, поради което информацията не може да се изтрие, или носителят е за еднократен запис, той се унищожава, без да се извършва специално изтриване. Специалното изтриване на информация или унищожаване на носители със записана класифицирана информация се извършва от комисия,

назначена със заповед на ръководителя на организационната единица, за което се изготвя протокол. Този протокол се подписва от членовете на комисията, предоставя се на служителя по сигурността на информацията и се съхранява в регистратурата. Той е основание за снемане от отчет на носителите в регистратурата и като материални средства.

Всички носители със записана класифицирана информация се преразглеждат периодично, за да се гарантира, че не се съхранява информация с по-високо ниво на класификация от обозначеното върху носителя. Контрол за наличността на носителите със записана класифицирана информация в организационната единица се извършва при проверките, извършвани по установения от нормативните документи ред.

Пренос на документи, съдържащи класифицирана информация, от една АИС или мрежа към друга се извършва само ако получателят е АИС или мрежа, сертифицирана за ниво на класификация на информацията, същото или по-високо от нивото на класификация на пренасяните документи.

Материалните носители на класифицирана информация, използвани в АИС или мрежи, се маркират, регистрират и съхраняват по начин, съответстващ на грифа за сигурност на носителя. Регистрирането, маркирането, контролът и унищожаването на материалните носители за многократен запис на класифицирана информация се извършват по предварително определен ред.

Информацията и материалите, осигуряващи достъп до ресурсите на АИС или мрежата, се защитават с мерки, съответни на мерките за най-високото ниво на класификация на информацията, за която дават достъп.

Информацията и материали, които вече не се използват за осигуряване на достъп до ресурсите на АИС или мрежата, се унищожават в съответствие с правилата в експлоатационната документация по сигурността и по начин, недопускащ възстановяване на информацията.

Преносими компютърни устройства, използвани за създаване, обработване и съхраняване на класифицирана информация, се разглеждат като носители на такава информация. Пренасянето на устройствата извън зоните за сигурност се извършва по реда на ППЗЗКИ.

Комуникационна и криптографска сигурност, защита от паразитни електромагнитни излъчвания

Комуникационната сигурност представлява система от мерки за сигурност, прилагани с цел защита на класифицираната информация от нерегламентиран достъп при нейното пренасяне по комуникационни системи. Тази система включва защита с криптографски методи и средства, защита от излъчвания и защита при пренасяне на информацията.

Комуникационните системи за пренос на класифицирана информация трябва да осигуряват механизми за:

1. надеждна и защитена идентификация и автентикация на изпращача и на получателя на информацията, които да се извършват преди началото на преноса на информацията;

2. осигуряване на конфиденциалност, интегритет и достъпност на пренасяната информация;

3. потвърждаване на получаването на информацията.

В АИС или мрежи се прилагат само криптографски средства, одобрени по установения ред.

Класифицирана информация се пренася по комуникационни системи извън зоните за сигурност на АИС или мрежи, когато е защитена с криптографски средства. Форма на информация, получена чрез обработка на класифицирана информация с одобрени криптографски средства, не представлява класифицирана информация.

Автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и/или пренася класифицирана информация с ниво на класификация „Поверително“ и повисоко, трябва да са осигурени срещу паразитни електромагнитни излъчвания, които могат да доведат до нерегламентиран достъп до информацията. Мерките за защита от електромагнитни излъчвания съответстват на най-високото ниво на класификация на информацията в АИС или мрежата.

Минимални изисквания за компютърна сигурност

Компютърната сигурност представлява система от мерки за сигурност, прилагани с цел осигуряване на конфиденциалност, интегритет и достъпност на класифицираната информация в АИС или мрежата. Тези мерки за сигурност се реализират чрез възмож-

ностите на техническите и програмните средства на компютърните системи и на специализирани средства. Минималните изисквания за компютърна сигурност на АИС или мрежа включват:

1. Еднозначна идентификация и автентикация на потребителя, които трябва да предхождат всички останали негови действия в АИС или мрежата;

2. Контрол на достъпа по преценка – осигуряване на достъпа до обектите на АИС или мрежата чрез предоставяне на права за достъп на базата на идентификацията на потребителя или неговата принадлежност към потребителска група; правата за достъп се предоставят само от упълномощени потребители или от администратора по сигурността на АИС или мрежата; механизмите за контрол трябва да осигуряват възможност за разделяне на потребителите и за достъп до информацията според принципа „необходимост да се знае“;

3. Непрекъснат запис на събития, свързани със сигурността на АИС или мрежата (одитни записи); записват се всички действия, свързани с контрола на достъпа, включително неуспешни опити за достъп, създаване или разрушаване на обекти или действия на оторизирани субекти, влияещи на сигурността на информационната система;

4. Възможност за изучаване на одитните записи и установяване на свързаните със сигурността действия на отделните субекти на АИС или мрежата;

5. Обработка на обекти на АИС или мрежата така, че при следващото им разпределяне към субект на АИС или мрежата той да не може да установи предишното им съдържание или да получи права за достъп на използвалите ги преди това субекти;

6. Защита от вредни програмни средства.

За осигуряване на минималните изисквания за сигурност се реализират програмни и технически механизми, спрямо които трябва да се осъществява конфигурационен контрол и които трябва да са защитени от нерегламентиран достъп.

Режими за сигурност

Автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и/или пренася класифицирана информация, се експлоатират в един или няколко от следните режими за сигурност:

1. „С общ достъп“;
2. „С общо ниво“;
3. „С много нива“.

При работа на АИС или мрежа в режим за сигурност „С общ достъп“:

1. всички потребители имат разрешение за достъп до най-високото ниво на класификация на информацията, която се създава, обработва, съхранява или пренася в АИС или мрежата;

2. всички потребители са упълномощени да работят с цялата класифицирана информация.

Компютърната сигурност за АИС или мрежа се осигурява с минималните изисквания за компютърна сигурност, като правата за достъп до обектите се предоставят само от администратора по сигурността на АИС или мрежата. При работа на АИС или мрежа в режим за сигурност „С общ достъп“ цялата информация, създавана, обработвана, съхранявана или пренасяна в АИС или мрежата, се защитава като информация с най-високо ниво на класификация, освен ако е налице гарантиран механизъм за разпознаване на нивото на класификация на информацията.

При работа на АИС или мрежа в режим за сигурност „С общо ниво“:

1. всички потребители имат разрешение за достъп до най-високото ниво на класификация на информацията, създавана, обработвана, съхранявана или пренасяна в АИС или мрежата;

2. достъпът на потребителите до класифицирана информация, за която те имат разрешение, се осъществява съгласно принципа „необходимост да се знае“.

Компютърната сигурност за АИС или мрежа се осигурява с минималните изисквания за компютърна сигурност.

При работа на АИС или мрежа в режим за сигурност „С общо ниво“ цялата информация, която се създава, обработва, съхранява или пренася в АИС или мрежата, се защитава като информация с най-високо ниво на класификация, освен ако е налице гарантиран механизъм за разпознаване на нивото на класификация на информацията.

При работа на АИС или мрежа в режим за сигурност „С много нива“:

1. не всички потребители имат разрешение за достъп до класифицирана информация с най-високо ниво на класификация;

2. достъпът на потребителите до класифицирана информация, за която те имат разрешение, се осъществява съгласно принципа „необходимост да се знае“;

3. компютърната сигурност за АИС или мрежа по ал. 1 се осигурява с минималните изисквания за компютърна сигурност и прилагане на задължителен контрол на достъп на субектите до обектите на АИС или мрежата.

Задължителният контрол на достъпа трябва да осигурява:

1. Присвояване на атрибут за сигурност на всеки субект и обект на АИС или мрежата; сравняването на атрибутите за сигурност на субектите с атрибутите за сигурност на обектите е основа за решения при осигуряване на достъпа;

2. Изключително упълномощаване на администратора по сигурността на АИС или мрежата за присвояване и изменение на атрибутите за сигурност на субектите на АИС или мрежата по реда, установен в документите по сигурността на АИС или мрежата;

3. Упълномощаване на определени потребители да присвояват атрибути за сигурност на входящи обекти, ако те не са притежавали такива атрибути;

4. Способност да се обозначи класификационното ниво на изходящия от АИС или мрежата обект на базата на неговия атрибут за сигурност;

5. Разпределяне на предварително дефинирани стойности на атрибутите за сигурност на новосъздадени обекти и съхраняване на атрибутите за сигурност при копиране на обекти;

6. Защита на интегритета на атрибутите за сигурност.

Сигурност по време на експлоатацията и развитието на сертифицирани АИС или мрежи

Експлоатацията и развитието на сертифицирана АИС или мрежа се извършват в пълно съответствие с установените мерки и процедури за сигурност и при съблюдаване на условията за нейното допълнително акредитиране. Органът по развитие и експлоатация, служителят и администраторът по сигурността, в рамките на своите отговорности, контролират и оценяват всички промени в глобалната, локалната и електронната среда за сигурност на АИС или мрежата и съвместно предлагат изменение на мерките и процедурите за сигурност. Когато промените не налагат изменение на

специфичните изисквания за сигурност, изменението на мерките и процедурите за сигурност се извършва с документ, утвърден от ръководителя на организационната единица, който става част от документите по сигурността на АИС или мрежата. Когато промените налагат изменение на специфичните изисквания за сигурност, те и описанието им се представят за утвърждаване от органа по акредитиране на сигурността на АИС или мрежи, който в срок определени работни дни след представяне на необходимите документи ги утвърждава или прави мотивиран отказ. Промените не се извършват преди утвърждаването им. Когато промените налагат допълнително акредитиране за сигурност на АИС или мрежата, се разкрива процедура по установения ред.

По време на експлоатацията и развитието на АИС или мрежата:

1. се извършва проверка на програмни средства и преносими носители на информация за наличието на вредни програмни средства, преди те да бъдат използвани в АИС или мрежата;

2. се извършва резервиране на системната и класифицираната информация, като резервните копия се съхраняват по начин, недопускащ нерегламентиран достъп до тях;

3. се извършват инсталиране на одобрени елементи и конфигуриране на АИС или мрежата само от оторизирани служители на организационната единица или от доставчика на АИС или мрежата под контрола на администратора по сигурността;

4. се извършва внедряване на нови технически и програмни средства или на техни версии само след оценка и тестване за сигурност от органа, работещ по сигурността, или след одобряване от орган по акредитиране на сигурността на АИС или мрежи, когато е необходимо допълнително акредитиране на АИС или мрежата;

5. се организира и извършва сервизна дейност по начин, недопускащ компрометиране на сигурността на АИС или мрежата;

6. се извършва ремонт на криптографски средства по установения от нормативните документи ред;

7. се извършва повторно одобряване за електромагнитни излъчвания на преминали ремонт технически средства;

8. не се допуска използване на носители на информация, технически и програмни средства, които са лична собственост.

Преносими компютърни устройства, съдържащи класифицирана информация, може да бъдат свързвани към АИС или мрежа

само ако тя е сертифицирана за ниво на класификация на информацията, съответстващо на маркировката на устройствата. В тези случаи служителят по сигурността на информацията на организационната единица дава разрешение за свързването. Преносимите компютърни устройства работят в места с осигурени мерки за физическа сигурност, съответстващи на нивото на класификация на информацията, съдържаща се в тях.

Сигурност на АИС или мрежи, в които се създава, обработва, съхранява или пренася информация с класификационно ниво „Строго секретно“

Класифицирана информация с класификационно ниво „Строго секретно“ се създава, обработва и съхранява в:

- автоматизирани информационни системи, изградени на базата на самостоятелни, несвързани в мрежа компютърни устройства, защитени от паразитни електромагнитни излъчвания, или
- автоматизирани информационни системи или мрежи, изградени в зони за сигурност, които са защитени от паразитни електромагнитни излъчвания.

Класифицирана информация с ниво на класификация „Строго секретно“ не се пренася по комуникационни системи извън зоните за сигурност. Класифицирана информация с класификационно ниво „Строго секретно“ не се обработва с преносими компютърни устройства.

АИС или мрежи, в които се създава, обработва, съхранява или пренася информация с ниво на класификация „Строго секретно“, работят в експлоатационен режим за сигурност „С общо ниво“. Те не могат да бъдат свързвани с други АИС и мрежи.

Криптографски методи и средства за защита на информация с ниво на класификация „Строго секретно“ може да се използват само за защита при съхраняване на информацията с цел прилагане на принципа „необходимост да се знае“.

Носителите за многократен запис на информация, използвани за съхраняване на информация с ниво на класификация „Строго секретно“, се водят в отделен регистър. Върху носителите за многократен запис с ниво на класификация „Строго секретно“ не може да се записва информация с по-ниско ниво на класификация. При изтичане на експлоатационния период на носителите за многокра-

тен запис с ниво на класификация „Строго секретно“ те не се декласифицират, а се унищожават. Повредените компютърни носители с ниво на класификация „Строго секретно“ не се ремонтират, а се унищожават по установения ред.

Възможност за заместване на мерките за компютърна сигурност

В случай на прекомерни разходи за осъществяване на някои мерки за компютърна сигурност те може да се заместят с мерки от другите видове сигурност на АИС или мрежа. В тези случаи се спазват следните принципи:

- Заместваната мярка за сигурност трябва да се реализира напълно;
- Качеството и нивото на заместваната мярка за сигурност трябва да бъдат запазени.

СИГУРНОСТ В КОМПЮТЪРНИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ ПРИ БЕДСТВИЯ, АВАРИИ И КАТАСТРОФИ ПРИ ВРЪЗКИ С ИНТЕРНЕТ

Възможности и риск

Предоставяната чрез интернет голяма гама от нови ресурси, нови видове услуги и свързаност внася както нови възможности, така и нови рискове. В отговор на рисковете тази политика описва официалната политика на организационната единица относно сигурността при връзка с интернет.

Не се допуска включването на АИС или мрежи, предназначени за създаване, обработка, съхраняване и пренасяне на класифицирана информация, към публични мрежи, като интернет и други подобни електронни комуникационни мрежи.

Приложение: Тази политика важи за всички работници (служители, партньори, консултанти, временно назначени лица и др.), които използват интернет чрез АИС или мрежи на организационната единица. На тези АИС или мрежи не може да се създава, съхранява, обработва, ползва и обменя класифицирана информация

От всички интернет потребители се очаква да са запознати и да спазват тук описаната политика. Въпросите по отношение на тази по-

литика трябва да бъдат отправяни към служителя или администратора по сигурността на АИС или мрежи. Нарушения на тази политика могат да доведат до анулирането на системните привилегии и/или предприемането на дисциплинарни действия, включително уволнение.

Предшестващо одобрение от ръководството: Достъпът до интернет (освен електронната поща) се предоставя само на тези служители, които имат легитимна нужда от такъв достъп, свързана с функционалните им задължения. Възможността за сърфиране в Мрежата и включване в други интернет дейности не е привилегия, валидна за всички служители. Служителите, на които ще бъде предоставен интернет достъп, трябва да са запознати със политиките за информационна сигурност.

Информационна цялост. Надеждност на информацията

Цялата информация, която се получава от интернет, трябва да се смята за подозрителна, освен ако не е потвърдена от отделна информация от различен източник. В интернет няма процес на качествен контрол и значителна част от информацията там е остаряла или не е акуратна, в някои случаи дори е преднамерено заблуждаваща. Съответно, преди да се използва безплатно доставена информация от интернет за целите на вземането на сериозни решения, служителите трябва да проверят информацията, като се консултират с други източници.

Проверка за вируси

Всички нетекстови файлове (бази данни, софтуерен код, таблици, архивирани файлове и т.н.), свалени от източници, които не са на организацията, по интернет, трябва да бъдат сканирани със софтуер за разпознаване на вируси, преди да бъдат използвани. Когато на външния източник на софтуера не може да се има доверие, сваленият софтуер трябва да бъде предварително изпробван на отделен компютър, който не се използва и на който наскоро е направено архивиране на информацията. Ако в този софтуер има вирус, червей или троянски кон, щетите ще бъдат нанесени само на тази машина. Свалените файлове трябва да бъдат декриптирани и декомпресирани, преди да се сканират за вируси. Отделно се препоръчва употребата на електронни подписи, за да има гаранция, че

информацията не е била променяна от неоторизирани лица. Това обаче не гарантира, че информацията е освободена от вируси.

Технологии за автоматично обновяване

Автоматичното обновяване на софтуер или информация на компютрите на организацията чрез интернет технологията „бекграунд пуш“ е забранено, освен ако включената система първо не е тествана и одобрена от дирекцията. Въпреки че тази нова технология е силна и полезна, тя може да бъде използвана за разпространяването на вируси или за причиняването на други операционни проблеми, като изваждане на цялата система извън употреба.

Snoop (навиране на носа) на потребители

Освен ако не се използват инструменти като електронен подпис и сертификати, е сравнително лесно да се подмени идентичността на друг потребител в интернет. Преди служители да направят достояние каквато и да е вътрешна информация на организацията, да създадат някакъв контакт или да поръчат каквито и да било продукти чрез публичните мрежи, идентичността на индивидите или организациите, с които се установява връзка, трябва да бъде потвърдена. Потвърждението на идентичността е най-добре да се изпълнява чрез дигитални подписи или дигитални сертификати, но в случаите, в които те не са налични, трябва да бъдат използвани други средства, като писма за кредит, референции от трети лица или телефонни разговори.

Анонимност на потребителя

Погрешно представяне, неизвестна идентичност, потискане или заменяне на идентичността на потребител в интернет или в каквито и да било електронни комуникации на организацията са забранени. Потребителското име, адресът на електронната поща, организационната принадлежност и свързаната информация, включена в съобщенията или пощата, трябва да отразяват действителния инициатор на съобщенията или пощата. Ако потребители имат нужда да използват ре-мейл или други анонимни средства, те трябва да правят това в своето лично време, със своите собствени информационни системи или със своите собствени акаунти за интернет достъп. Употребата на анонимно FTP свързване, анонимно UUCP свързване, HTTP браузване и други методи за достъп, осъществени, очаквайки, че потребителите са анонимни, е позволена.

Java

Всички интернет потребители трябва да направят негодно ползването на Java, като променят конфигурацията по подразбиране на своя интернет браузър софтуер. Благонадеждни механизми, които да предпазят от нанасяне на щети на системите, софтуера и данните на организацията при използването на Java (както и на ActiveX и други подобни програми), все още няма в наличност. Използването на Java (или подобни програми) на системата на организацията е забранено, освен ако предварително не са дадени специални права от интернет групата на Отдела за информационни системи.

Промяна на уеб страници

Служители не могат да изграждат нови интернет страници, свързани с организацията, или да правят промени на съществуващи уеб страници, свързани с организацията, освен ако нямат предварително одобрение от Комитета за интернет мениджмънт. За промени се смятат прибавянето на връзки към други сайтове, обновяването на показаната информация и изменянето на графичния изглед на страница. Този комитет трябва да бъде сигурен, че материалът, който ще бъде изложен там, има логичен и добър вид, съответства на целите на организацията и е защитен с адекватни мерки за сигурност.

Конфиденциалност на информацията. Размяна на информация

Според споразуменията за конфиденциалност, подписани от всички служители, софтуерът, документацията и всякакъв друг вид вътрешна информация не трябва да бъдат предавани или по друг начин отдавани на други лица, които не са част от организацията, за други цели освен такива, които са изрично определени от ръководството. Размени на софтуер и/или данни между организацията и трети лица не трябва да има, освен ако не е подписано предварително споразумение. Подобно споразумение трябва да определя условията за размяна, както и начините, по които софтуерът и/или данните трябва да бъдат третирани и защитени. Редовните процедури – като изпращане на продукт в отговор на клиентски ордер – не трябва да включват подобни специфични споразумения, след като сроковете и условията се подразбират.

Материали, изпращани по пощата

Служителите не трябва да изпращат некриптирани материали на организацията (софтуер, вътрешни бележки, политики и т.н.) на какъвто и да е компютър с публичен достъп до интернет, който поддържа анонимно FTP или подобни услуги за публичен достъп, освен ако изпращането на тези материали не е предварително одобрено от директора на публичните връзки. Общо казано, вътрешната информация на организацията не трябва да бъде поставяна на който и да е компютър, освен ако лицата, имащи достъп до този компютър, имат легитимна „нужда за знание", отнасяща се до съответната информация.

Подслушване на съобщения

Подслушването на съобщения е открито и често срещано в интернет. Съответно секретната, собствената или личната информация на организацията не трябва да бъде изпращана чрез интернет, освен ако преди това не е била криптирана чрез одобрените методи за криптиране. Освен ако не се знае, че е в публичния домейн, сорс кодът трябва винаги да се криптира, преди да бъде изпратен чрез интернет. Поради същите причини услугите, предлагани в интернет за телефонни разговори, не трябва да бъдат използвани за целите на организацията, освен ако не се знае предварително, че връзката се криптира.

Параметри за сигурност

Номера на кредитни карти, номера на карти за телефонни обаждания, фиксирани пароли за предоставяне на достъп и други параметри за сигурност, които може да бъдат използвани за предоставяне на достъп до продукти или услуги, не трябва да бъдат изпращани в интернет в четима форма. И двата процеса на криптиране – SSL и SET, са одобрени стандарти за криптиране в интернет за защита на параметрите за сигурност. Други процеси на криптиране, като PGP, са позволени, ако са одобрени от началника на информационната сигурност.

Публично представяне. Външно представяне

Служители могат да посочват своята принадлежност към имейл списъците (listservs) на организацията, чатсесии и други предлагани в интернет услуги. Това може да се направи чрез изрично прибавяне на определени думи или може да се подразбира, например чрез електронна поща. И в двата случая, когато служителите покажат принадлежност към организацията, те трябва също така ясно да посочат, че изразеното мнение е тяхно лично, не е задължително да е на организацията. Подобно, ако е показана принадлежност към организацията, изявления, защитаващи различни политически сили, и предоставянето на продукти/услуги също са забранени, освен ако не са предварително уточнени с отговарящия за публичните изявления.

Подходящо поведение

За да се избегнат дискредитиране, оклеветяване на даден човек или други легални проблеми, когато съществува принадлежност към организацията, добавена към интернет съобщение или имейл, клевети или подобни писмени атаки са строго забранени. Подобно, служители не трябва да заплашват друг потребител или организация чрез интернет. Всички интернет съобщения, целящи да тормозят, безпокоят или тревожат други лица, също са забранени.

Отстраняване от имейл списък

Съобщения, които са изпратени на интернет групи за дискусии, електронни бюлетини, табла или други публични форуми и включват косвена или категорична принадлежност към организацията, може да бъдат премахнати, ако ръководството смята, че не противоречат на интересите или съществуващите политики на организацията. Съобщенията, спадащи към тази категория, включват:

- Политически изявления;
- Религиозни изявления;
- Използване на неприличен език (ругаене);
- Изявления от типа „тормоз“ – базирани на раса, вяра, цвят, години, пол, физически увреждания или сексуална ориентация.

Решението да се премахне електронната поща, трябва да бъде взето от началника на информационната сигурност или директора

на „Човешки ресурси“. Когато това е практически осъществимо, лицата, отговорни за тези съобщения, ще бъдат информирани за решението и ще им бъде предоставена възможност да премахнат съобщението (съобщенията) сами.

Разкриване на вътрешна информация

Служителите не трябва публично да разкриват чрез интернет вътрешна информация на организацията, която може да повлияе на договори, връзки с трети лица (клиенти, партньори и др.) или може да попречи на публичното им представяне, освен ако няма одобрение на директора на публичните връзки или член на главното ръководство. Подобна информация включва проспекти, продукти в процес на проучване или разработка, анализи за представянето на дадени продукти, дати за появяването на продукти на пазара, вътрешни проблеми с информационните системи и др. Отговори на специфични имейли, изпратени от клиенти, са изключения от тази политика.

Неумишлени разкрития

Коментарите и въпросите, изпращани на имейл списъците (listservs), публични news групи, Usenet и подобни публични съобщения в интернет трябва да се структурират правилно. Преди някакъв материал да бъде изпратен, служителите трябва да вземат под внимание това дали информацията няма по някакъв начин да навреди на организацията или дали материалът няма да причини проблеми от типа на публични връзки. Служителите трябва да имат предвид, че няколко отделни „отрязъка“ информация може да бъдат свързани в едно от вражески настроени лица, за да се формира картина, разкриваща конфиденциална информация, която след това да бъде използвана срещу организацията. Въпреки че може да изглежда различно от преобладаващата интернет култура на откритост, за да се избегнат тези проблеми тип „мозайка“, служителите трябва да бъдат по-скоро резервирани, отколкото „на разположение“ с вътрешната информация на организацията.

Права на интелектуална собственост

Организацията поддържа стриктно придържане към споразумения за софтуерни лицензи с продавача. Когато се използват компютърните или мрежовите ресурси на организацията, строго се

забранява копиране на софтуер по начин, който не съответства на лицензa на продавача. Участие в извънработните часове в бюлетини, табла за пиратски софтуер и други подобни дейности са в конфликт с интересите на организацията и също са забранени. Репродукцията, изпращането или по друг начин преиздаването или преразпределението на думи, графики или други материали следва да бъдат извършвани само с позволението на автора/собственика. Служителите трябва да приемат, че всички материали в интернет са с права, освен ако има специално съобщение, което казва друго. Когато информация от интернет е интегрирана във вътрешни доклади или използвана за други цели, целият материал трябва да включва обозначения като „Всички права са запазени“, както и детайли за източника на информацията (имена на автора, URL адреси, дати и др.).

Публично използвани директории

Всички публично използвани директории на компютрите на организацията, които са свързани с интернет, трябва да бъдат разглеждани и изчиствани всяка вечер. Този процес е нужен, за да се предотврати анонимната размяна на информация, несъобразена с дейностите на организацията. Примерите включват пиратски софтуер, откраднати пароли, откраднати номера на кредитни карти и неподходящо написан или неуместен графичен материал (например порнография). Служители, използващи компютрите на организацията, не трябва да бъдат свързвани по какъвто и да било начин с размяната на материала, описан по-горе.

Контрол на достъпа. Връщане на потребителската автентичност

Всички потребители, желаещи да установят връзка в реално време с вътрешните компютри на организацията чрез интернет, трябва да удостоверят автентичността си на firewall, преди да получат достъп до вътрешната мрежа на организацията. Този процес на удостоверяване на автентичността трябва да бъде постигнат чрез система за динамични пароли, одобрена от началника на информационната сигурност. Примери за одобрени технологии включват смарткарти с динамични пароли и „прозрачни за потребителя“ системи за противопоставяне или отзвук. Тези системи възпрепятстват

нарушителите да познаят фиксирани пароли или повторно да използват фиксирани пароли, които са били разпознати по време на sniffer атаки (wiretrap). Определени „публични“ системи (анонимно FTP, уеб сърфиране и т.н.) нямат нужда от процес на удостоверяване на автентичността, защото се очакват анонимни взаимодействия.

Браузър за потребителска автентичност

Потребителите не трябва да записват фиксирани пароли на своите уеб браузъри или имейл клиенти, защото това ще позволи на всеки, който има физически достъп до тяхната работна станция, да има достъп до интернет с тяхната идентичност, както и да чете и да изпраща от тяхната електронна поща. Вместо това тези фиксирани пароли трябва да бъдат предоставяни всеки път, когато е изпратена заявка към браузър или имейл клиент. Браузърните пароли може да бъдат записвани само ако boot паролата трябва да бъде предоставяна всеки път, когато системата не е активна за определен период от време.

ISPs

С изключение на телекомите и потребителите на мобилни компютри служителите не трябва да си служат с интернет сметки и комутируеми линии, с които да влизат в интернет от компютрите на организацията. Вместо това цялата интернет дейност трябва да минава през firewall на организацията, така че да може да бъдат прилагани контролът на достъпа и свързаните с това механизми.

Създаване на мрежови връзки

Освен ако не е получено предварителното одобрение на началника на телекомуникационните услуги, служителите не могат да установяват интернет или други връзки с външни мрежи, които могат да позволят на потребители, които не са служители на организацията, да имат достъп до системите и информацията на организацията. Тези връзки включват създаването на мултикомпютърни файлови системи (например NIS на компанията Sun), уеб страници, интернет системи за комуникация, FTP сървъри и други подобни.

Създаване на нови служебни канали

Освен ако VP на информационните системи, VP на маркетинга или главният съвет не са одобрили предварително, на служителите

се забранява да използват нови или вече съществуващи интернет връзки, за да създават нови бизнес канали. Тези канали включват EDI (Разменяне на електронни данни) споразумения, електронни канали за онлайн пазаруване, онлайн услуги за бази данни и др.

Лично ползване

Служители на организацията за управление на насърчаването, които имат даден интернет достъп, могат да сърфират в интернет за лични цели само в личното, а не в работното си време. Подобно, игри, нюс групи и други дейности, които не са свързани с работата, трябва да бъдат извършвани в личното време. Използването на компютърните ресурси на организацията за тези лични цели е позволено дотолкова, доколкото стойността на това ползване е минимална и доколкото дейността на организацията не е оставена на заден план. Служителите не трябва да използват интернет или други вътрешни информационни системи по начин, който да пречи на продуктивността на другите служители; примерите включват верижни писма и разпространяване на молби за благотворителност.

Спиране на сайтове

Firewalls на организацията рутинно пречат на потребители да се свързват с определени уеб сайтове, които нямат връзка със служебната работа. Служители, които използват компютрите на организацията и открият, че са се свързали с уеб сайт, съдържащ сексуално съдържание, расистка, насилническа или друга потенциално оскърбителна информация, трябва незабавно да прекъснат връзката си с този сайт. Възможността за свързване с определени уеб сайтове сама по себе си не означава, че на потребителите на системите на организацията е позволено да посещават такива сайтове.

Лични очаквания. Без защита по подразбиране

Служителите на организацията, използващи информационните системи на организацията и/или интернет, трябва да осъзнаят, че техните комуникации не са автоматично защитени да не бъдат разглеждани от трети лица. Освен ако не се използва криптиране, служителите не трябва да изпращат чрез интернет информация, която смятат за конфиденциална или лична.

Преглед от ръководството

По всяко време и без предварително предупреждение ръководството на организацията си запазва правото да преглежда електронната поща, файлове на персоналните компютри, cache файловете на уеб браузър, отбелязани уеб страници, логове на посетени уеб страници и друга информация, записана или минаваща през компютрите на организацията. Подобен достъп на ръководството обезпечава съответствието с вътрешните политики, спомага на вътрешните разследвания и асистира при управлението на информационните системи на организацията.

Логване

Организацията рутинно записва посещаваните уеб сайтове, свалените файлове, времето, прекарано в интернет, и друга подобна информация. Началниците на отдели получават доклади за тази информация и я използват за определяне на това какъв тип използване на интернет е подходящ за дейностите на техния отдел.

Джънк поща

Когато служителите получават нежелана или непоискана поща (известна и под името spam), те трябва да се въздържат от отговаряне на директния подател. Вместо това трябва да изпратят съобщението/писмото до имейлният администратор на организацията, който да предприеме стъпки за прекратяването на по-нататъшни трансмисии.

Докладване на проблеми със сигурността. Процес на уведомяване

Ако чувствителна информация на организацията е изгубена, разкрита на неоправомощени лица или се подозира нейното разкриване или изгубване, началникът на информационната сигурност трябва да бъде уведомен незабавно. Ако информационните системи на организацията се използват неоправомощено или се предполага такова използване, началникът на информационната сигурност трябва да бъде уведомен незабавно. Също така, когато пароли или други системни механизми за контрол на достъпа са изгубени, откраднати или разкрити или пък се подозират такива действия, началникът на информационната сигурност трябва да бъде уведо-

мен незабавно. Това трябва да се направи, защото може да означава, че е станало заразяване с компютърен вирус. Подобни проблеми със сигурността, необичайно поведение на системата, като липсващи файлове, чести системни сривове, пренасочени съобщения и др., също трябва да бъдат незабавно докладвани. Спецификата на проблемите на сигурността не трябва да бъде дискутирана открито, а да бъде споделяна на базата на „нужно знание".

Фалшиви доклади за сигурност

Интернет е нападнат от фалшиви съобщения, заявяващи различни проблеми със сигурността. Много от тези измами вземат формата на верижни писма, които изискват от получателя да изпраща съобщения на други хора. Служители, имащи информация за системната уязвимост, трябва да я предоставят на началника на информационната сигурност, който да определи какви действия да се предприемат. Служителите не трябва лично да преразпределят информация за системната уязвимост.

Контрол върху тестването

Неоторизирани служители не трябват да проучват механизмите за сигурност на организацията или други интернет сайтове, освен ако нямат предварително одобрение от началника на информационната сигурност. Ако механизмите за сигурност са проучвани от служители, то без да има нужда, ще бъдат задействани аларми и ще бъдат ненужно изразходвани ресурси за следене на дейността.

ХИБРИДНИ ВОЙНИ И „ЦВЕТНИ" РЕВОЛЮЦИИ
Кой разбърква боите и кои са художниците?

Още в самото начало на този раздел бих желал да изразя категоричното си становище, че напоследък терминът „хибридна война" се експонира в публичното пространство повече, отколкото е необходимо. Не само Общата информационна среда, но и Специализираните (частни) информационни среди се характеризират със засилено и тенденциозно информационно пресищане, свързано с „експлоатацията" на тази специфична терминология. Създава се впечатлението, че не само доморасли политици, но и „пишман специалистите" по сигурност за щяло и не щяло използват термина

„хибридни войни“, за да скрият своята дразнеща некомпетентност. По този повод ми се ще да цитирам анализатора Боян Чуков, който каза: *„Самото понятие „хибридна война“ е „семантичен локум“. Можеш да го разтягаш както си пожелаеш.*

В арсенала на хибридната война влизат всички некинетични оръжия, които могат да измислят хората. Конфликтите в нея са „течни конфликти“. Тоест те нямат определена форма и могат да преминават от един в друг. За хибридната война, както и за тероризма, няма общоприета дефиниция. Мисля, че едно определение може да бъде: „Хибридната война е безпределната същност на международните некинетични стълкновения“. Хибридната война има политически, икономически, културни, исторически, спортни, дипломатически и всякакви други проекции. Тя може да бъде водена и под благородния лозунг за борба с корупцията. Например, след като корумпираш управляващите в дадена страна, започваш да преследваш селективно само тези, които са се отклонили от правилната посока на зададения предварително геополитически вектор. Ако управляващите не слушат, моментално външният фактор организира regime change.

...Хибридната война е нещо много коварно. Насилието в нея може да се модулира. Да се разтяга във времето. Например с прилагането на икономически санкции. Коментатори говорят, че хибридната война не води до летален край на хората, но не е така. Погледнете Венецуела. Хора умират в болниците, бебета в родилните домове. Гладът в резултат на икономически санкции също убива, но разтеглено във времето. Въобще „хибритизирането“ свидетелства само за промяна в характера на войната, но не и на нейната същност. Хибридната война размива границата между времето на мир и времето на война. ...Хибридната война е като понятието „глобална война с тероризма“. ***И двете понятия се превърнаха в политически щампи.*** *И двете можеш да ги използваш както си искаш. Особено днес, когато международното право е отдавна в реанимация.*

...За първи път понятието „хибридна война“ се появява през 1998 г. в докторатата на Робърт Уолкър и през 2002 г. в разработките на Уилям Немет. И двамата са от Морското училище в Калифорния. Те теоретизират преминаването на американската армия в Ирак през 1990 г. от регулярни в нерегулярни методи. Тео-

ретизират за дифузията между основните методи на война – регулярни и нерегулярни. През 2005 г. Франк Хофман и Джеймс Матис отново ползват израза „хибридна война“. През 2014 г. хибридната война придоби съвсем нов смисъл. Тя беше преоткрита отново като катализатор за колективната защита в НАТО. Хибридната война и „руската хибридна заплаха“ послужиха като мотив за реинтегрирането на страните членки на НАТО в съюза“ (http://epicenter.bg/article/Boyan-Chukov--Evropeytsite-sa-zalozhnitsi-na-amerikanskata-PRO-/181328/11/34).

Хибридната война се определя от Военната доктрина на САЩ като използване на две или повече от следните средства за въздействие върху противниковата страна:

- Военна сила;
- Държавни паравоенни сили (като силите за вътрешна сигурност, полицията или бреговата охрана);
- Революционни организации (движения, които основно разчитат на подривна дейност и насилие, за да променят статуквото);
- Партизански отряди;
- Престъпни организации.

Казано по друг начин, най-често под „хибридна война“ се разбира използването на (не)конвенционални средства за постигане на военната цел – унищожаване, дестабилизация или превземане на противника. Някои известни специалисти в областта на сигурността не са съгласни с тази дефиниция. Те смятат например, че всяка съвременна война е по същността си хибридна и подобни дефиниции, като психологическа война, хибридна война, партизанска война, единствено пречат да се осъзнае тяхната същност. Както пише Колин Грей (Colin S. Gray, “Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context”), „според Клаузевиц, Сун Дзъ и Тукидид общата теория за войната и стратегията за нейното водене е теория с универсално приложение. Множеството начини за водене на война и използването на различни стратегически средства не са от никакво значение за естеството на войната“.

Теория и практика на хибридната война

След цитирането на Боян Чуков нека още веднъж да си зададем въпроса: Какво представлява всъщност „хибридната война“? Много хора бързат да поставят знак на равенство между нея и т.нар. „асиметрична война“. На практика обаче хибридният подход към войната е следващата стъпка в еволюцията на въоръжените конфликти. За нея започва да се говори някъде в средата на миналото десетилетие. Конфликти от този тип, от една страна, съчетават конвенционални методи на водене на военни действия, а от друга, използват и невоенни средства за постигане на конкретни политически цели.

Прилагането на хибридни стратегии и тактики не е някаква военна или политическа новост. Масовизирането им обаче нарасна значително след края на Студената война, когато в повечето случаи воденето на конвенционални войни в крайна сметка носи катастрофални последици и за държавата агресор. Затова в много от случаите формално недържавни формирования се използват като камуфлаж от страната – инициатор на хибридната атака. Както и асиметричната, хибридната война няма ясно очертана „фронтова линия“. Тя се води с ограничени военни и всички невоенни средства на няколко условни бойни полета – в „конфликтната зона“, сред населението и на ниво международна общност, където преди всичко се търси естествена или принудена легитимност. Може би най-важната характеристика на хибридната война е съчетаването на ограничени военни и пълен набор невоенни действия за постигането на поставените преди всичко политически цели. По този начин не само държавата – цел и обект на неформална агресия, но и международната общност до последния момент трудно могат да кажат с достатъчна увереност дали срещу съответната държава се води координирана офанзива, или не. А дори и да са наясно с това, тайният характер на хибридните стратегии и тактики не дава достатъчно легално основание на държавата – цел, да отвърне със сила или да иска помощ от своите съюзници. Този извод се подсилва и от факта, че в някои от случаите използването на невоенни средства за натиск и налагане на политическа воля не означава непременно, че тези действия имат за цел да провокират някаква форма на реален въоръжен конфликт, а не са просто форма на брутална и агресивна дипломация.

Ескалацията на хибридните заплахи до реални въоръжени конфликти води до извода, че ключовият елемент за тяхното противодействие трябва да бъдат специалните служби.

Концепция за хибридната война

Както вече обърнахме внимание, концепцията за хибридната война не е нито политическа новост, нито някакво ново откритие на военните стратези. Тя е просто естествена еволюция на войната.

Във връзка с това беше създадена стратегията за изпреварващ, превантивен удар за борба с тероризма и всеобхватен подход на НАТО към операциите. НАТО прие и концепция за противодействие на хибридните заплахи, в която се съобщава, че те могат да задействат чл. 5 от Договора за колективна отбрана.

В бившия Съветски съюз (респективно в Русия) хибридната война е описана още през 50-те години на XX век в книгата на полковник Е. Едуардович „Метежна война“[7]. През последните години пак там бе разработена и използвана в реалната политическа практика т.нар. концепция за „меката сила“.

През 1999 г. Китайската народна република „прие на въоръжение“ асиметрична стратегия, наречена „неограничена война“ (буквално „война без граници“), която включва бойни действия във всички съвременни пространства на бойното поле.

В съвременния глобален свят комбинирано се използват „мирни“ и военни средства за постигане на желаните политически цели. Военните стратези и експертите по сигурността описват новия начин на водене на война с термина **„война на контролирания хаос“**.

Цел на хибридната война

В теоретичен и най-вече в практически план всички военни доктрини се фокусират върху задачата за потискане на волята на врага, като подчиняването му е средство за постигане на целите. Затова най-важната задача в хибридната война е въздействието върху масовото съзнание на обществото, както и съзнанието и реалните действия на определени държавни и обществени лидери, отговорни за вземането на важни политически решения.

Оттук произтича и основната цел на хибридната война – с всички възможни средства и по всякакъв начин силово да се завзе-

ме властта в държавата – цел, за да се извърши преразпределение на нейните ресурси, както и преразпределение на социалните роли от новата, **поставена** власт в интерес на друга държава или група от държави.

Не само в западните, но и в източните военни традиции всяка война не е непременно свързана с използването на смъртоносни и разрушителни оръжия за избиване на живата сила на противника или за унищожаване на неговата инфраструктура. По същество тези традиции следват класическата мисъл на Клаузевиц: „Войната е акт на насилие, който има за цел да накара врага да изпълнява нашата воля".

Методи на хибридната война

Може да се диференцират няколко основни метода за водене на хибридна война:

- Въоръжени действия чрез традиционен сблъсък със смъртоносни и разрушителни оръжия;
- Провеждане на (дез)информационни операции;
- Провеждане на психологически операции;
- Тотално използване на кибератаки за нарушаване на държавното и местното управление, гражданската критична инфраструктура, военното командване и управление и логистичната поддръжка;
- Екстремна конфронтация в областта на дипломацията;
- Финансова и икономическа война;
- Използване на социално-психологически и политически „аргументи";
- Идеологически сблъсък на културно и религиозно ниво;
- Жестоко технологично противоборство;
- Целенасочено въздействие върху поведението на големи групи от хора, които са потенциални източници на заплаха в държавата – цел;
- Местни граждански конфликти, съпроводени с терористични атентати, масови кланетата, грабежи, „организирана" престъпност и насаждане на страх;
- Тотална въоръжена борба срещу всички несъгласни под лозунга на борба със съществуващия недемократичен режим или лидер;

• Изостряне на отношенията между гражданите на държавата – цел, и правителството.

Характеристики на хибридната война

След преглед на различни източници и на основата на анализ на конкретни ситуации в различни краища на света можем да диференцираме следните **основни характеристики на хибридната война**:

• Хибридната война представлява сблъсък на културно ниво за правото на съществуване на определен социум;

• Хибридната война има **глобален характер**. Тя се води навсякъде по света;

• Хибридната война има постоянен и **универсален характер**, тъй като е в ход постоянно увеличаване на интензитета на всички фронтове и театри на „бойните“ действия. Във връзка с това е необходимо армиите да бъдат в постоянна готовност за всякакво развитие на ситуацията, навсякъде по света, с всякаква възможни военни съюзи и формати. В същото време видът на въоръжените конфликти ще зависи главно от промените в геополитическата среда, причинени от борба за власт и ресурси;

• Хибридната война има... **хибриден характер**, тъй като се използват всички познати днес средства – от най-старите примитивни методи до най-новите и сложни методи за водене на война;

• Хибридната война има **дифузен характер**. Дифузните войни не са случайни. Те са планирани и най-важното – добре организирани;

• Хибридната война има **всеобхватен характер**; инвазията е от типа „**мрежова война**“, няма контролен център;

• При хибридната война **недържавните сили са срещу всички институции на държавата**;

• Хибридната война масово използва **(дез)информационните** и психологическите операции;

• При хибридната война се наблюдава тотално използване на всички видове **тероризъм** като част от общата стратегия за постигане на целите.

Алгоритми за провеждане на хибридни войни

Общият алгоритмичен механизъм на хибридната война може да се изгради в следната последователност:

I ФАЗА

Първата фаза започва с „помощ“ от неправителствени организации (НПО) в държавата – цел. Това по същество би могло да бъдат различни антиправителствени „граждански“ организации или етнически групи, които приканват населението да вземе нещата в свои ръце срещу правителството под прикритието на патриотични подбуди. Предвижда се използването на естествените в такива ситуации **слабости на институциите**, недоволството на местните общности, на малцинствени групи и граждански движения, за да се създаде объркване сред населението на държавата – цел. Чрез провеждането на психологически операции се манипулира поведението на определена социална група с цел нейната радикализация.

Друга основна технология в тази фаза са (дез)информационните операции за постигане на пълно информационно превъзходство. За тази цел тотално се манипулират или в крайна сметка дори насилствено се купуват водещи телевизии, радиа, вестници, списания и уеб сайтове. **Манипулирането на общественото мнение** цели да се задълбочат различията между обществото и управляващите, а така също да се разколебаят евентуалните съюзници на държавата – цел. Всичко това се подкрепя с предизвикване на икономическа криза, например чрез вдигане на цените на енергоносителите или намаляване на туристическите потоци. В случая трябва да се отчита и нарастването на ролята на разузнавателните централи и техните контакти с организираната престъпност или нарочно радикализирани групи или лица.

При тази ситуация не само е желателно, но и задължително правителството на държавата – цел, да вземе адекватни мерки за гарантиране на сигурността на населението си.

II ФАЗА

Действията при **тази фаза** започват с организирането на антиправителствени демонстрации, митинги и екстремни протести, които прерастват в открити бунтове. Атакуващата държава по всякакъв начин ще насърчава провеждането на демонстрации, протести и **митинги,** докато обстановката ескалира неконтролируемо. В повечето случаи протестните действия ескалират светкавично и довеждат до внезапна смяна на управляващия режим в държавата – цел. Практиката показва, че почти винаги държавата – цел, се до-

вежда до състояние на тотална катастрофа.

Горните събития се осигуряват на първо място чрез засилена употреба на **социалните мрежи**.

III ФАЗА

Третата фаза продължава с **действия във военната област** чрез интензивно провеждане на военни учения и съсредоточаване на войски. Подготовката за военни действия от страна на атакуващата държава се съчетава с извършване на чести провокации в граничните зони и засилване на информационните операции срещу държавата – цел. Под прикритието на операции за доставка на хуманитарни помощи (?) се правят опити да се транспортират допълнителни военни сили за установяване на пълен контрол над страната. В края на тази фаза **целта е да се състави ново правителство**, което да се признае от световната общественост.

Христоматиен пример за подобно развитие на ситуацията, по всяка от трите фази, в нейната пълнота, са събитията във и около латиноамериканската държава Венецуела през пролетта на 2019 г.

Някои методи за борба с хибридната война

Основните методи, които биха могли да повлияят благоприятно на решаването на породената от хибридната война криза, са **политически диалог, осигуряване на подкрепа от международната общност, както и поддържане на подкрепата от населението на държавата – цел, за водената от правителството политика**.

Провеждането на информационни и други „специализирани“ операции за противодействие на противниковото влияние над морала и психиката на населението, въоръжените сили и силите за сигурност на държавата – цел, имащи за задача запазването на нейната национална идентичност и културните ѝ традиции, е базов метод за борба с хибридната война. Една от най-ефективните технологии при тази барба е постоянното провеждане на патриотично възпитание в обучението както на подрастващите, така и на всички граждани.

За предотвратяването на заплахата от вътрешна дестабилизация е необходимо превантивно унищожаване на формиращите се бандитски структури и техните съучастници до началото на евен-

туалните активни бойни действия. Задължително трябва да се предотврати създаването на пета колона като организирана неконструктивна опозиция и да се унищожат създадените депа за оръжие и лагери за обучение. В случая е необходимо и превантивно унищожаване на всички финансови трансакции и информационни канали към противодействащите на законното правителство структури, както и всякаква чуждестранна помощ тях.

Освен това трябва да се обърне внимание на факта, че „военният елемент на хибридната заплаха е само малка част от цялостната стратегия и има смисъл само ако е интегриран и синхронизиран с всички останали невоенни елементи. Независимо от това адекватното противодействие на военния елемент лишава агресора от възможност за ескалиране на конфликта. В резултат се създават висока вероятност за ликвидиране на заплахата във фаза „възпиране“ и благоприятни условия за фазата „защита“ в хибридното противопоставяне“.

Една хибридна война може да бъде спечелена само ако:

- навреме се осъзнае, че това е война; в общия случай една такава война не се чувства осезаемо, но тя съществува;
- имаме предварително разработени собствени политики за водене на хибридна война;
- твърдо се ръководим от разбирането, че войната е стратегия, планиране, мобилизиране, и тази военна аксиома се прилага в текущата държавна политика и практика;
- подготвяме новото поколение да служи на отечеството и водим адекватна бойна подготовка на въоръжените сили;
- са налице политическо, икономическо и социално взаимодействие в провеждането на планирани превантивни защитни операции.

За съжаление, планиращите политически и военни стратези използват чисто военни методи и средства и нямат поглед върху цивилните аспекти, влияещи на набора от защитни операции. От държавническа гледна точка обаче, за да има успех, планирането трябва да бъде всеобхватно. Във връзка с това е добре да се включват специалисти от всички сфери на влияние и нива на планиране на операциите, както и да се развиват способности за водене на информационни и психологически операции и контраоперации. Задължително е при планирането в групите на стратегическо ниво

да има представители и на оперативното ниво, които да участват в съвместните дейности с цел да се съкрати движението на информация от зоната на операцията и да се вземат бързи и адекватни решения. На практика психологическите и информационните операции се провеждат само от гледна точка на стратегията поради обичайната централизираност на въоръжените сили. Оперативната гледна точка планира чисто военни операции, които не са относими към хибридната война.

В съответствие с практиката, че хибридната война обикновено се замисля от мирно време, най-голямата **заплаха за националната сигурност на страната** може да дойде поради следните причини:

- Липса на навременно разработване на подходящи планове;
- Липса на теории, стратегии и инструментариум за водене на специфични военни действия;
- Неотчитане на сериозността на създалата се ситуация;
- Липса на съвременно контраразузнаване;
- Липса на подходящи мерки за защита на критичната инфраструктура;
- Липса на заделяне на необходимите военновременни запаси, ресурси и средства както за предотвратяване, така и за водене на война;
- Липса на координация между различните държавни структури и органи;
- Националната икономика няма готовност за реакция в случай на криза.

Естествена и вътрешноприсъща характеристика на хибридните войни представляват т.нар. „цветни революции“.

ЩО Е ТО „ЦВЕТНА РЕВОЛЮЦИЯ“?

През втората половина на XX век се случиха няколко много силни обществено-икономически и политически сътресения, както и поредица от революционни вълни в различни региони на света. В този период са и така наречените „нежни революции“ от края на 80-те години в Източна Европа, вълната от „цветни революции“ в държавите от постсъветското пространство и не съвсем накрая – „революциите“, получили названието „Арабска пролет“, в държави-

те от Северна Африка. Между тях не може да се постави знак за равенство, но не може да се пренебрегне и фактът, че са налице редица сходства в начините на провеждането им. Дефинитивно доказателство за това е „успешно" реализираната през 2014 г. „надстройка" на украинската „Оранжева революция", етикетирана с добилото популярност наименование „Евромайдан". Това ни води до мисълта, че независимо в кой регион на света са държавите, станали обект на „революционни" действия, съществува сходен сценарий за провокирането и осъществяването на тези т.нар. революции.

„Цветна революция" е термин, с който е прието да се назовават редица обществено-политически събития по целия свят в края на XX и началото на XXI век. Това е технология за осъществяване на смяна на властта (държавен преврат) в определена страна, в която натискът върху управляващите се извършва под формата на политически шантаж чрез използването на инструмента протестно движение (в много от случаите – подчертано младежко). Характерните черти на „цветните революции" са масовите митинги и демонстрации, като целта е не просто смяна на настоящия политически елит и неговата геополитическа ориентация, а промяна на основата на цялата държавност. Военната сила не е основният инструмент на тълпите, които искат незабавна смяна на политическия режим. От гледна точка на успешното провеждане на този тип революция в основата на действията е да се изгради негативен образ на управляващите.

Моделът на цветните революции се състои от осем основни фази:[21]

1. Всяка „цветна революция" започва с тотална и масирана медийна подготовка с продължителност от един месец до една година;

2. Формира се организирано протестно движение, което е основната движеща сила на бъдещата „цветна революция";

3. Всяка демонстрация на това движение, преимуществено в един-два от най-големите градове на съответната държава, е съпроводена от инцидент, който шокира обществото и води до обществен отговор. Например в Тунис – държава с авторитарен режим,

[21] На основата на: **Манойло**, А., О. **Карпович**. Цветные революции – теория и практика демонтажа современных политических режимов. Юнити, 2015.

през 2010 г. започват демонстрации след самозапалването на млад търговец. Целта е да се привлече общественото внимание;

4. След такъв инцидент протестната мрежа излиза по улиците на големите градове, където групи активисти стават катализатори на стихийни масови процеси, които успешно въвличат широк кръг от хора;

5. Следващата фаза е да се създаде политическа „тълпа", и за това се избира достатъчно голямо по площ място, например известен за обществото площад, където да се събере огромна маса хора. В условията на създадената „тълпа" на определеното за това място, се наблюдава въздействие на подсъзнанието на отделната личност, като се внедряват нови „демократични" ценности (най-вече такива, прокламирани от САЩ и западните държави – демократични ценности);

6. От името на цялата тълпа се поставят ултимативни изисквания към управляващия елит;

7. Реално „придобиване" на властови ресурси;

8. Силна вътрешна и международна медийна защита на „постигнатото".

Разликата с традиционните революции е тази, че „цветните" революции са по скоро мрежови процес. Те възникват и се развиват в канали на средствата за масова информация (СМИ). По този начин може лесно и преднамерено да се оказва въздействие на отделната личност и на обществото. В определен смисъл този тип революции може да се разглеждат като някаква форма на информационно-психологическа война, тъй като същността ѝ се състои в скритото, тайно управление на политическите, военните, икономическите, социалните и т.н. процеси на държавата – потенциален противник, или на държавата, попадаща в дадена сфера на геополитически интереси.

Също така целта на информационната война е да оказва въздействие на знанията, представите и мислите на противника. Обект на „нападението" в информационната война са: информационната инфраструктура, съзнанието, волята, чувствата на населението, както и самото приемане на политически, икономически и социални решения в другата държава, особено в период на нестабилност или на кризисни ситуации. В случая с „цветните революции" сме свидетели имено на този акт: промяна и въздействие на мислите и съзнанието на обществото в държавата, както и форми-

ране на нов тип поведение – отхвърляне на статуквото, желание за нов тип обществено-политически отношения, в това число смяна на режима на управление.

С оглед на съвременните събития, протичащи на Европейския континент, а и в достатъчна близост до нашата страна, е необходимо да обърнем внимание на процесите в Украйна. Все още разпространеният термин „цветна революция" не е широко използван за действията в Киев, но се наблюдават редица прилики с други „цветни революции", състояли се по целия свят – в Грузия, Египет, а дори и „Оранжевата революция" в Украйна през 2004 г. Една от общите характеристики на украинската „революция" с другите такива е народното вълнение, което се превръща в масови безредици, характеризиращи се със стихийност на действията. Също така се наблюдава добре организирано протестно движение, което избира за свой „терен" Площада на Независимостта в Киев (и в този случай е налице фаза пет от основните осем фази на цветните революции, за които стана въпрос). Блокада и невъзможност за предприемане на каквито и да е действия от страна на действащия президент, е другата отличителна, но и обща черта на този тип революции. Целта на украинския народ, макар и в голяма степен разделен, е не само сваляне на тогавашния проруски настроен президент, а и промяна на геополитическата ориентация на страната.

„Цветните революции" в повечето случаи се провеждат в региони със стратегическо значение – притежаващи стратегически и природни ресурси (например богати на петрол), а също и в такива, попадащи в сферата на геополитическите интереси на някоя друга държава. Затова и намесата на външни за държавата субекти е неизбежна. За повечето изследователи на международните отношения, а също и за отделния индивид е ясно, че Украйна и нейният народ попадат в сферата на влияние на Руската федерация. Чрез предоставената възможност на Украинската държава да се обвърже икономически и търговски с Европейския съюз, се накърняват геополитическите интереси на Русия. Създава се една благоприятна „почва" за информационно противоборство, което, от една страна, е водено между поддръжници и опоненти на политическия режим в страната, а от друга страна, между външни за страната субекти, имащи отношение към тези протестни действия, в украинския случай – между западните страни, по-специално САЩ, и страните

от Европейския съюз и Руската федерация. В частност векторът на информационната политика на Европейския съюз е насочен към създаване на определени позитивни негови образи в съзнанието на чуждата аудитория, в съзнанието на украинското население, които са насочени към европейската интеграция на Украйна, като показват по негативен начин действията на руските власти. От своя страна Русия води информационна кампания, която е в противоречие с тази на ЕС. Руската федерация се стреми да създаде имидж на „закрилник“ на украинския народ, като пропагандира естественото историческо и културно минало на двата народа. И двете страни влагат много финансови и човешки ресурси за водените от тях информационни политики, които в голяма степен са насочени една срещу друга.

Кой разбърква боите и кои са художниците?

В основата на сценария на цветните революции е англосаксонската, в частност северноамериканската идеология за „промотирането“ и изнасянето към определени държави на демокрацията, на демократичните идеали и ценности. Тази теза се потвърждава и от едно изказване на президента на САЩ Джордж Буш, който навремето казваше, че „оцеляването на свободата в Америка зависи от успеха на свободата по други земи“!? „Цветните революции“ често са наричани инструмент на „меката сила“ (soft power), термин, въведен от Джоузеф Най.[22] Същността ѝ се състои в това да привличаш и убеждаваш чрез определени културни ценности и примери. Според Най „меката сила лежи върху способността да оформяш предпочитанията на другите чрез нематериални ценности, като култура, политически ценности, институции и политики, които са възприемани за легитимни. Главният смисъл е да се влияе на поведението на хората, като се заставят по несилов начин да направят нещо, което не биха направили до този момент“.

„Меката сила“ цели да спечели обществата и правителствата в другите държави на страната на този, който я прилага. Тя не се

[22] **Nye**, J. Soft Power: The Means to Success in World Politics. Chapter 4 - Wielding Soft Power, URL: http://belfercenter.hks.harvard.edu/files/joe_nye_wielding_soft_power.pdf

осъществява само от държавите, а и от всички други участници в международната политика. Трудно е обаче да определим „цветните революции“ като директен инструмент на soft power, тъй като тя се осъществява посредством различни мирни инициативи за изнасяне на ценности, а например в случая със Сирия се наблюдава обратното. Действията на САЩ и техните партньори в началото на конфликта се характеризираха по-скоро с принуждаване към демокрация, без да се отчитат и отстраняват първопричините за протичащите там политически, социални, етнически и верски конфликти, което доведе до ескалация и нагнетяване на напрежението, смъртта на повече от 200 хиляди души и неконтролираното бягство от страната на около 2 милиона сирийци.

Въпреки съществуващите различия в държавите, в които избухват „цветните революции“, например в икономическото и социалното развитие, геополитическото положение и т.н., ясно се вижда, че те „избухват“ по една и съща схема, по един сценарий. А именно: шаблонът на (младежко) протестно движение, преобразуването му в политическа тълпа и използването на тази сила против действащите политически власти. Това безспорно ни навежда на мисълта, че тези актове, насочени към промяна на статуквото, не са така стихийни и спонтанни, а всъщност са „режисирани“ от външен за страните субект.

Именно „цветните революции“ може да се разглеждат като създаване на нов световен ред – чрез промяна на ценностите в даден регион и въздействие върху отделните индивиди, които целенасочено биват подтиквани да желаят и да постигнат коренна промяна в обществено-политическата обстановка в страната си.

САЩ, в качеството си на велика сила, която притежава амбициите и възможностите да разпространява общоприети ценности, като демокрация, свобода и човешки права, е в основата на стратегиите за промяна на режимите в отделни страни по света. Докато за САЩ това е процес на разпространение на демократичните ценности и идеали, за Руската федерация това е скрита политическа тактика на САЩ и НАТО, която цели доближаването им до границите ѝ и създаване на сфери на влияние в региони, които са от стратегическо значение за Федерацията.

В западните медии „цветните революции“ станаха нарицателно име за борбата на обществата срещу авторитарните им управля-

ващи. „Цветните революции“ в Северна Африка, по-известни с наименованието „Арабска пролет“, са тясно свързани с реализацията на провъзгласената по времето на Джордж Буш програма за „промотиране“ на свободите в света. По този повод често от администрацията на президента се изтъкваше значимата роля на САЩ за демократизирането на различни части, региони и държави.

В своя реч и 44-тият президент на САЩ Барак Обама (2009 – 2017) заявява намерението на своята страна да подпомага всеки активист и организация, които отстояват демократичните ценности в страната си, и за това те ще могат да разчитат на подкрепа от всякакво естество от страна на американците.

Важен фактор в сценария на революциите заема американският институт „Алберт Айнщайн“ (Albert Einstein Institution – AEI), който е създаден от Джийн Шарп, известен със своя труд „От диктатура към демокрация“. Неговите текстове са добре изучавани от различни протестни граждански групи в Египет, Иран, Сърбия и др. Смята се, че именно неговите публикации помагат на опозицията и протестиращите да извършат (ненасилствена) смяна на управляващите. Разпространението на демокрацията посредством „цветните революции“ се осъществява и чрез Агенцията за международно развитие на САЩ (US Agency for International Development – USAID), чиято дейност е насочена към спазването на правата на човека, свободата на словото, провеждането на демократични избори и др.

Хаосът обаче, който съпровожда редица революции, най-вече става дума за тези в Северна Африка и изостилата се криза в Украйна през последната година, е един от най-сериозните глобални проблеми на това десетилетие. Израждането на движещите сили на тези т.нар. „революции“ в някои страни и региони в чисто фашистки формирования и антицивилизационни фундаменталистки ислямски орди определят усещането за нещо, което почти винаги излиза от контрола на своите създатели и в повечето случаи се обръща против тях. Въпреки това в частност Съединените американски щати и Обединена Европа разглеждат проблема Украйна като управляем и виждат в него ефективен инструмент за демократизация на съвременния свят.

Заключение

В условията на глобализация светът не става по-предсказуем и стабилен, а напротив. Той се характеризира с хаос и разрастване на междудържавните и вътрешнодържавните конфликти. Един от катализаторите на този хаос са т.нар. „цветни революции“, обхванали различни страни по света. Независимо дали са в постсъветското пространство, или в държавите от Северна Африка, те радикално променят картината на международните отношения. В крайна сметка това не е нещо ново. Още навремето Николо Макиавели съвсем аргументирано защитава тезата, че въоръжените конфликти и в частност войните не представляват драстично отклонение от нормалното човешко поведение. На основата на историческата статистика той доказва, че периодите на мирно развитие на човечеството са много по-кратки от периодите на война, независимо от това дали тя ще се води на бойното поле, на пазара, или в съвременния си вариант – пред компютрите.

Ролята на Запада, по-специално на САЩ, в т.нар. „цветни революции“ в различни региони е очевидна. САЩ е и държавата, която взема ролята на „върховен арбитър“ за разрешаването на проблемите на обществата, които по свое желание или не са тръгнали по пътя на демокрацията.

Идеята за глобално разпространение на демократично-либералните ценности, подкрепена с новите информационни и комуникационни технологии, способства за целенасочено, активно и тайно въздействие на съзнанието, мислите и действията на народите в регионите, обхванати от „цветните революции“. Бързо и лесно се променят историческата и културната памет, възприемат се нови ценности и норми на поведение. И... в крайна сметка светът се променя!

Като обобщение на тази тема може да се каже, че хибридните заплахи са едни от най-опасните съвременни предизвикателства пред сигурността и отбраната и ако не се предприемат подходящите контрамерки, те могат да доведат до пълно цивилизационно и културно изтриване на заплашената държава от лицето на света.

КИБЕРСИГУРНОСТ

Киберсигурност – концепции, политики и стратегии[23]

Историята на киберсигурността започва с изследователски проект. Робърт (Боб) Томас, изследовател от Кеймбридж, Масачузетс, осъзнал, че е възможно компютърната програма да се движи в Мрежата, оставяйки малка следа, където и да отиде. Той нарекъл тази програма „Пълзящо растение“ (Creeper) и я проектирал да се придвижва между терминалите на TENEX[24] от началото на ARPANET[25], отпечатвайки съобщението „Аз съм пълзящото растение. Хвани ме, ако можеш“. Друг изследовател на име Рей Томлинсън (човекът, изобретил имейла) видял тази идея и я харесал. Той си „поиграл“ с програмата и я превърнал в самопроизвеждаща се – първия компютърен червей. След това написал друга програма – „Жътвар“ (Reaper), първия антивирусен софтуер, който ще преследва „Пълзящото растение“ и ще го изтрие.

Странно е да погледнем назад от позицията, в която се намираме сега, в епохата на вируси като „Рансъмуер“ (Ransomware), зловреден софтуер и нападения на национални държави, и да се запитаме как стигнахме дотук.

От академично начало – бърз ход към престъпността. През поголямата част от 70-те и 80-те години заплахите за компютърната сигурност са били ясни. Но тези заплахи са били под формата на злонамерени вътрешни лица, чели документи, които не би трябвало да четат. Следователно практиката на компютърна сигурност, която се върти около управлението на риска и съответствието, се развива отделно от историята на софтуера за компютърна сигурност.

Проблемите в Мрежата и злонамереният софтуер са съществували и са били използвани за злонамерени цели още по време на ранната история на компютрите. Руснаците например бързо започнали да използват киберсилата като оръжие. През 1986 г. гер-

---

[23] Моноскрипт на дисертационен труд с автор Кристина Босакова.

[24] Tenex – операционна система от 1960 г.

[25] ARPANET е първата в света функционираща компютърна мрежа от вида комутация на пакети по протокол TCP/IP, предшественик на интернет.

манският компютърен хакер Маркус Хес хакнал интернет портал в „Бъркли“ и използвал тази връзка, за да „стъпи на гърба“ на тогавашната операционна система ARPANET. Той разбил 400 военни компютъра, включително мейнфреймите (централните процесори) в Пентагона, с намерението да продаде тайните си на КГБ. Той бил хванат едва когато един астроном на име Клифърд Стол открил проникването и разгърнал техниката на име „гърнето с мед“ (the honeypot technique)[26].

В този момент в историята на киберсигурността компютърните вируси започнали да стават по-малко академични и по-скоро сериозна заплаха. Увеличаването на мрежовата връзка означавало, че вируси като червея почти били унищожили ранния интернет, което започнало да стимулира идеята за създаването на първия антивирусен софтуер и защитата в киберпространството.

Киберпространство

Днес терминът „киберпространство“ се използва в много контексти, но невинаги е ясно какво точно описва и какво означава. Причината, поради която се избира терминът „киберпространство“, е, че всички други термини (например: киберсигурност, киберпрестъпност, кибервойна, кибертероризъм и т.н.) възникват в самото киберпространство. Следователно киберсигурност е сигурността на киберпространството.

Киберпрестъпността е престъпност, извършена в киберпространството или там, където елементи от киберпространството се използват като средство за извършване на престъпление.

Терминът „киберпространство“ често се използва взаимозаменяемо с „интернет“ по отношение на интернет културата, интернет приложенията и т.н. Навлизането на интернет и доставката на жични/безжични мрежи са създали киберпространството. В киберпространството хората се смятат за по-равни и действат поразлично, отколкото в реалния свят, защото онлайн обществото се състои от непостоянни идентичности на индивиди и несъвпадане

[26] Honeypot е механизъм за компютърна сигурност, създаден да открива, отклонява или по някакъв начин да противодейства на опитите за неразрешено използване на информационните системи.

на социалната и политическата йерархия с реалното пространство. Киберпространството като цяло е интерактивна комуникационна среда, чрез която всеки, който има достъп до нея, може широко и незабавно да разпространява и получава идеи и мнения за конкретни цели. По тази причина киберпространството е признато за важна област с улеснен бърз обмен на информация (14).

В реалния свят съществуват недостатъци, така че трябва да се очаква, че и киберпространството ще има такива. Това се дължи главно на факта, че реалният свят и киберпространството са обитавани от едни и същи хора.

В киберпространството липсват национални граници или законодателни разпоредби, а при съвременните възможности на технологиите се улеснява достъпът както на легитимни субекти, така и на лица, групи, институции или държави с разнородни цели. Така силно се увеличава неговата уязвимост, особено през интернет, което позволява извършването на широк спектър от нерегламентирани дейности. Те може да бъдат от най-дребните и безобидни, като кражба на лични данни, подправяне или злоупотреба с тях, включително с цел реализиране на финансови облаги, до целенасочени атаки за блокиране на елементи от критичната национална или международна инфраструктура, нарушаване или блокиране на системите за управление в критични области на обществения живот, добиване на класифицирана разузнавателна информация и др.

Може да се приеме условно, че **киберпространството** е цялата област от информационни ресурси, налична чрез компютърни мрежи. В него първоначално се влага изцяло технологичен смисъл и то включва всички елементи на компютърни системи, мрежи и технологии, както и съществуващите информационни масиви. Но още при изграждането на това пространство започват да се появяват редица предизвикателства, свързани с циркулиращата цифровизирана информация. Първоначално тези рискове и проблеми, както и необходимостта от гарантиране на сигурност се обсъждат в тесен кръг от технически експерти, предимно на национално ниво.

С времето на множество народи стана известно, че макар киберпространството да предлага много ползи, то носи и редица последици за безопасността и сигурността. Впоследствие прилагането на култура за киберсигурност все повече се превръща в гло-

бална надежда и желание. За съжаление, в момента липсва добре дефинирано и очертано определение на самото културно направление за киберсигурност.

Киберсигурност

Киберсигурността от много години е грижа и отговорност на всички участници в киберпространството. В стремежа да се намалят киберрисковете, към сигурността на технологиите бяха насочени мерки, които бяха смятани за крайни и достатъчни. Днес обаче се възприема, че процесът по осигуряване на киберсигурност изисква много повече от обикновен технически контрол, а именно човешки ориентиран подход и най-вече изграждане на **култура на киберсигурност**. Въпреки че ролята на формирането на култура за надеждно киберпространство е добре осъзната, изследванията, фокусирани върху културата на киберсигурността, все още са в начален стадий.

Киберсигурността е активността по защита на информацията и информационните системи (мрежи, компютри, бази данни, центрове за данни и приложения) с подходящи процедурни и технически мерки за сигурност.

Националната инициатива за кариери и изследвания в областта на киберсигурността в своя речник определя киберсигурността така: „Дейността или процесът, умението или способността, или състоянието, при които информационните и комуникационните системи и информацията, съдържаща се в тях, са защитени от увреждане, използване без разрешение или променяне“.

Голяма част от кибератаките срещу информационните системи и данните, съхранявани в тях, са престъпления с цел финансови облаги. Други форми на престъпления в киберпространството са тормоз, измама, разпространение на детска порнография, нарушаване на правата на интелектуалната собственост и др. За престъпниците използването на киберпространството за осигуряване на материални блага изглежда привлекателно поради възможността за отдалечен достъп и сравнително ниската сложност на извършваните в него престъпления.

Ресурсите, отделяни за осъществяването на действия в киберпространството, целите, поставяни за изпълнение, и важността на предприеманите действия са гаранция за разгръщането на сериоз-

ни конфликти без ясно обозначени географски граници, без физически допир, с много мощен потенциал за деструктивно въздействие върху човечеството.

Противодействието срещу киберпрестъпността се усложнява от разнообразието на атаките, очакваните поражения и мотивацията на хората, извършващи атаките. Мотивацията може да варира от преследване на икономически облаги до чисто любопитство или хулиганство. В последните години действията на киберпрестъпниците са далеч по-изтънчени поради придобитите значителни ресурси, усъвършенстването на организационните структури и разпределението на задачите между криминалните мрежи. Атаките през интернет са систематични и често са насочени към високостойностни, но не добре защитени цели.

В киберпространството всички заинтересовани страни трябва да имат активна роля за защита на собствените си активи. Основното изискване в киберпространството към физическите лица и организациите е готовност при възникване на заплахи за сигурността за ефективното им неутрализиране и адекватна реакция на нарушения, злоупотреби и престъпна дейност. Всички заинтересовани страни следва да предприемат подходящи мерки за установяване и поддържане на сигурност в киберпространството.

Киберсигурността се базира на: информационната сигурност, сигурността на приложенията, мрежовата сигурност и сигурността на интернет, като на стълбове на своя фундамент. Киберсигурността е важен компонент на информационните системи за защита на ключови обекти от критичната информационна инфраструктура. В същото време адекватната защита на обектите от критичната информационна инфраструктура (т.е. гарантирането на тяхната безопасност, надеждност и достъпност) служи за целите на киберсигурността.

Уникалността на киберсигурността се проявява в ролята на заинтересованите страни, чиято дейност е свързана с поддържане и подобряване на сигурността на киберпространството като цяло.

„Киберсигурност“ не е синоним на „информационна сигурност“, тъй като те се различават по обхват.

Точното определение на „киберсигурност“ все още се обсъжда активно в изследователската общност. Някои автори използват „киберсигурност“ взаимозаменяемо с „информационна сигурност“

(Астахова, 2014; Гернаути-Хели, 2009). Една от срещаните дефиниции определя киберсигурността като защита и запазване на конфиденциалността, целостта и достъпността (CIA) на информацията, което е предимство в сферата на киберпространството (IEC 27032 / IEC 27032, 2012).

Поверителност означава, че информацията е достъпна само за оторизирани потребители. Интегритетът се стреми да гарантира, че информацията е непроменена, надеждна и пълна. И накрая, наличието се отнася до наличието на информация винаги за оправомощени потребители (Conklin and White, 2006).

Дефиницията за киберсигурност се свързва директно с тази за информационна сигурност, която е „запазване на поверителността, целостта и наличието на информация“ (IEC 27032 / IEC 27002, 2005). Информационната сигурност има за цел да осигури непрекъснатост на бизнеса и да ограничи въздействието на инциденти по сигурността, за да се сведат до минимум бизнес вредите (von Solms and van Niekerk, 2013). Като такава, информационната сигурност се занимава основно със запазването на информация в контекста на организацията.

Киберсигурността обаче се простира далеч отвъд границите на бизнеса, като се има предвид, че информацията се споделя и използва в киберпространството. Следователно, въпреки наличието на тясна връзка между информационната сигурност и киберсигурността, съществуват аспекти, които попадат извън обхвата на информационната сигурност (von Solms and van Niekerk, 2013).

Според von Solms и van Niekerk (2013) киберсигурността се определя като: защитата на самото киберпространство, електронната информация, информационните и комуникационните технологии, които поддържат киберпространството и потребителите на киберпространството в личен, обществен и национален план, включително всеки от техните интереси, материални или нематериални, които са уязвими за атаки, идващи от киберпространството.

Термините, свързани със сигурността, се променят през годините, тъй като лидерите на общността на информационната сигурност разгърнаха термините за управление на информационната сигурност през осигуряването на информация в дневния ред, включително в настоящия си вид на киберсигурност, специално обръщайки внимание на електронните аспекти. Въпреки това це-

лите винаги са били едни и същи, а именно да защитаваме основно информацията, която обработваме и за която сме отговорни. Също толкова важно е, че липсва разбиране в рамките на общността на сигурността по отношение на това какво всъщност е киберсигурност. Например Health Information Trust Alliance посочва, че „киберсигурността не се занимава с участието на незлонамерена човешка заплаха, като добронамерен, но заблуден служител".

Независимо от огромното нарастване на интереса и приемането на управлението на информационната сигурност, включително на киберсигурността, все още има пропуски и слабости в рамките на индустрията и практиката. Това се вижда от големия брой значими инциденти в областта на сигурността и нарушенията на данните, които се публикуват редовно, включително неотдавнашните инциденти през 2018 г.:

- Една от „най-скъпите" кибератаки до момента, NotPetya – криптовирусът „разкъса" компании от цял свят, причинявайки загубата на терабайти чувствителна информация;
- Атаката на ирански хакери срещу университети в САЩ. След като осъществяват атака срещу над 300 университета в САЩ, група ирански хакери биват разпознати и осъдени. В процеса се стига до заключението, че са успели да проникнат в 144 университета в САЩ, 176 университета в 21 други страни и 47 частни компании. Според Министерството на правосъдието на САЩ хакерите са откраднали над 31 терабайта данни;
- Сред случаите с най-много медийно внимание попада и този на фирмата Exactis – компания, събираща лични данни, които може да бъдат използвани за изнудване. Доскоро тя ги е съхранявала на публично достъпни сървъри;
- Фитнес тракер стана източник на 150 милиона потребителски записа. Атаката над MyFitness Pal е отличен пример за неспособността на корпоративния свят да навакса с изискванията на сигурността. Източването на данни тук се случва единствено защото част от тях са криптирани с доказано уязвим алгоритъм – SHA1. Другата част от данните са надеждно подсигурени и не пострадват при атаката.

В резултат на продължаващото докладване и публикуване на тежки нарушения в организационната и личната сигурност организациите и потребителите все повече се фокусират върху търсе-

нето на начини за подсигуряване, за да защитят своята марка и репутация, както и да предотвратят или намалят свързаните с това финансови последици. Това създава представа за неспособността на настоящите методи за осигуряване както на промишлеността, така и на обществото. Необходими са технологии и подходи за осигуряване в допълнение към технологиите, които ще защитят организациите и обществеността като цяло от продължаващи скъпи нарушения в киберпространството. Такъв вид решение можем да намерим в изграждането и повишаването на културата на киберсигурността на потребителите в киберпространството.

Киберсигурност – важност и необходимост

Днешният ни начин на живот фундаментално зависи от интернет. Въпросите, свързани с киберсигурността, които произлизат от нашата технологична зависимост, засягат буквално всички хора.

„В нашето дигитално време въпросите на киберсигурността не засягат само хората от технологичните среди, те засягат всички нас – без значение дали работиш в сферата на бизнеса, или на политиката, на армията, или на медиите, или си просто гражданин“ (Ерик Шмид, изпълнителен директор (CEO) на Google).

Киберсигурността е тема, която вълнува цялото ни общество, тъй като то става все по-зависимо от глобалната информационна и комуникационна инфраструктура, но като всяко общо благо, киберпространството доказано може да се използва като поле за злоупотреби (19). Повечето развити икономики днес са изцяло зависими от уеб базирани услуги и подкопаването на увереността в тези системи и мрежи може да нанесе огромни вреди.

Въпросите за киберзащитата, изграждането на национални органи в областта на устойчивата киберсигурност, изработването на правила за общоевропейска реакция при киберкризи и провеждането на съвместни учения бяха сред най-важните теми по време на Българското председателство на Съвета на ЕС през 2018 г.

Киберпрестъпления – предизвикателства, заплахи и рискове

В съвременните изследвания по въпросите на сигурността съществува определен консенсус за класификацията на вредните въздействия на средата върху субекта. Авторът на книги и топексперт в областта на военното дело и сигурността Димитър Йончев ги свежда до три: предизвикателства, заплахи и рискове. Предизвикателството е определено като „състояние на средата на сигурност, което предполага някакъв отговор". То може и да не бъде забелязано или да бъде изтълкувано погрешно. Заплахата е също състояние на средата, когато тя е норма, но това състояние се вижда с просто око. „Рискът е заплаха с неустановен срок." Под „риск" разбираме вероятността дадена заплаха да се превърне в потенциална уязвимост и резултатно въздействие от неблагоприятното събитие върху личността. Вероятността за възникване на заплаха от определен източник е свързана с определена уязвимост на информационните технологии, комбинирана с нивото на въздействието (риск) и подготовката на потребителя.

Рискът се свързва и с доверието, което е важна концепция, свързана с управлението на риска. Отношението към доверието влияе върху поведението във вътрешните и външните взаимодействия, като основни елементи са:

- Концептуални начини на мислене или възприемане на доверието;
- Надежност;
- Как надеждността влияе върху изграждането на доверие.

Доверието е вярата, че един елемент ще се държи по определен – предвидим, начин, при определени обстоятелства. Елементът може да бъде човек, процес или обект. От гледна точка на надеждността това е атрибут на лице, което осигурява увереност у другите за възможностите си.

В контекста на сигурността на информационните технологии заплахите може да се дефинират като вътрешни или външни действия или събития, които могат да причинят вреди на системите, приложенията или информацията на организация. „Вътрешни или външни" означава, че опасността може да идва отвътре или извън организацията. Това може да причини неупълномощено разкриване, преместване, разрушаване или унищожаване на информация и

системи. Computer Emergency Response Team (CERT 1993) дефинира заплахата като „всякакви обстоятелства или събития, които могат да навредят на система или мрежа“. Също така заплахите може да се разделят на физически или киберзаплахи. Физическите заплахи увреждат машините и връзките (унищожаване на съоръженията за комуникации). От друга страна, киберзаплахите идват от лица с добри компютърни умения, които злонамерено използват приложения под формата на вируси, червеи, троянски коне или атакуващи скриптове. Установено е, че киберзаплахите могат да причинят по-големи вреди от физическите. Възприятието почти винаги изостава от реалността. Когато става дума за приемане на истини, които не променят нашия погрешен начин на мислене, инерцията е просто част от човешката природа, но това може да бъде опасно. Въпреки че физическите заплахи за бизнеса могат да бъдат много сериозни, онлайн заплахите са много по-разпространени и имат непосредствено въздействие върху приходите. Киберпробивът или лошият репутационен рейтинг онлайн има по-голяма вероятност да навредят на приходите и дори да затворят бизнес, отколкото един грабеж. Разбираемо е защо собствениците на предприятия се страхуват да не станат жертви на влизане с взлом и грабеж, дори в проучване на компанията Womply[27] за заплахи за малкия бизнес 52% от респондентите обявяват, че именно кражбата и грабежът биха били „изключително тежки“ за техния бизнес. Истината е, че кражбите или грабежите са доста редки и стават все по-лесни за предотвратяване. Според данни на Insureon[28] по-малко от 9% от малките и средните предприятия са били жертва на обир или кражба. Освен това повечето кражби в бизнеса включват служители, а не маскирани бандити, които разбиват и грабят. За разлика от физическите заплахи онлайн заплахите са по-неприятни и опасни, защото са по-трудни за предотвратяване и причиняват по-драматични спадове в приходите. Като цяло собствениците на бизнес не разбират онлайн бизнес заплахите и не знаят как да за-

[27] Womply е компания, която е партньор в платежната индустрия с цел да даде възможност на малките фирми да използват технологии и данни.

[28] Insureon е търговска застрахователна агенция и посредник, която улеснява малкия бизнес, независимите предприемачи и независимите изпълнители да намират търговска застраховка.

щитят своите компании от тях. Въпреки разпространението на кибератаките сред малките фирми собствениците не признават сериозността им. Според същото проучване на Womply едва 32% от респондентите смятат, че кибератаката е „изключително вредна", класирайки я извън първите 10 отговора и под варианти като „трудова злополука на служител". Това е стряскащо тревожно, тъй като 60% от малките предприятия, които са се сблъсквали с кибератака, са излезли от бизнеса в рамките на шест месеца.

Различното възприятие на риска, познавателните способности и персоналните характеристики са човешки фактори, които играят значителна роля в информационната сигурност. Всички те си взаимодействат и могат да доведат до поведение, което вреди на информационната сигурност.

Киберпрестъпници

Понякога те се крият точно под носа ни: колега зад близкото бюро, студент в университета или просто случайно лице с лаптоп в кварталното кафене. Съответно на икономическото си въздействие киберпрестъпността се превърна в оръжие на терористични групи и национални държави, което повишава потенциалната опасност до наистина кошмарни нива. Разследващият репортер Брайън Кребс, автор на KrebsOnSecurity.com[29], обрисува стряскащ портрет на организирани международни престъпни кибергрупи, действащи нагло и с чувство за безнаказаност, който би накарал дори Ал Капоне да завижда.

За **хакер** се приема лице, притежаващо умението да проникне без разрешение в компютърните данни и системи на друго лице с цел извличане на полза. Тази полза или цел не трябва да се възприема по подразбиране, че е злонамерена, тъй като различните типове хакери имат различни мотиви.

Хакери. Диференциация

• *White hat* – лица, чиито действия не са насочени към нанасяне на вреда; когато действието се осъществява със знанието на собственика и без нанасяне на вреда; обикновено това са хора с

[29] KrebsOnSecurity.com, ежедневен блог за компютърна сигурност и киберпрестъпност.

добри компютърни умения, работещи в областта на компютърните технологии и имащи за цел да откриват слабите места в компютърните системи; често биват наемани като консултанти и експерти за повишаване на сигурността във фирмени ИТ системи;

• *Black hat* – това са злонамерени лица, които проникват незаконно в компютърните системи с цел измама, кражба, пиратство и т.н.; намеренията им са деструктивни, без знанието на собственика и с вредоносна цел (наричат се и кракери);

• *Grey hat* – хакери, които не са злонамерени, но могат да извършат пробив в компютърните системи с цел печалба, самодоказване или изява; с цел да покажат на администраторите къде има пробиви, но и да припечелят от това;

• *Elite/White hat* – тези хакери представляват най-високото ниво в хакерското общество; интелигентността им е висока, притежават социална компетентност, въпреки че са по-скоро интровертен тип личности, успяват добре да контролират емоционалните си състояния и нивата на стрес; лесно се приспособяват към новите ситуации, имат висок праг на търпимост и добре развито аналитично мислене; често пъти престъпленията, извършени от тях, имат нарцистичен характер, който индикира наличието на високо его, затова водещи **мотиви** за този тип престъпления са предимно предизвикателството и себеизявата.

В доклада „Интелигентни методи и киберсигурност“ са посочени и описани петте поколения на киберпрестъпниците:

Първото поколение на престъпните действия в киберпространството се характеризира с бързо размножаване на червеи, които експлоатират разпространените уязвимости. За киберпрестъпниците от това поколение приоритет № 1 е да бъдат забелязани.

Отличителната черта на киберпрестъпленията от второто поколение е мотивът за печалба. Ботнетите (големи мрежи от заразени компютри) се превърнаха в предпочитано оръжие за киберпрестъпниците, позволявайки им да „изпомпват“ милиони спам съобщения или да извършват атаки от типа „разпределен отказ на услуги (DDoS – Distributed Denial of Service)“ върху бизнеса или администрациите.

Две отличителни черти притежава третото поколение киберпрестъпления: организация и дискретност. Киберпрестъпниците осъзнават предимствата на съвместната работа за незаконни доходи.

Възникването на дейността „C2C (Criminal-to-Criminal)“ дава началото на четвъртото поколение на киберпрестъпността. Появява се силна и ефективна сива икономика, която предоставя на киберпрестъпниците възможности да купуват и продават стоки и услуги един на друг. Отделни специализирани киберпрестъпни бизнеси станаха известни.

Заплахите в петото поколение са все по-автоматизирани, като започват да се ползват от предимството на инструменти и техники за писане на скриптове за автоматизиране на различни етапи на своите схеми. По-малко опитни хакери могат да закупят инструменти за лесно идентифициране на уязвими цели, за компрометиране на системи и за кражба на данни. В някои случаи, при по-големите схеми за престъпления в киберпространството, се наблюдава интеграция в рамките на няколко комплекта инструменти, които изпълняват различни функции (25).

От злонамерените хакери най-често срещаните са измамниците и крадците на финансови средства. Измамата и кражбата на финансови средства като компютърно престъпление се отнася към злоупотребата с данни или лични сметки с цел приемане на чужда самоличност и извършване на незаконни действия. При разпространяването на зловреден софтуер съществуват три основни мотива на този тип извършители на компютърни престъпления: вреда и разрушаване на компютърната система, кражба/измама, извличане на информация. Целите им биват: финансови облаги, отмъщение и изява. Този тип нарушители притежават изкривена самооценка, неувереност в себе си, нестабилност на егото, чувство за непълноценност, липса на социални умения. Друг основен мотив са отмъщението, реваншът и вандализмът, подтикващи към използването на зловреден софтуер.

Както вече казахме, за достъп до важни данни е необходима автентикация. Известни са три основни начина за автентикация:

- Нещо, което потребителят знае (като парола или ПИН);
- Нещо, което потребителят притежава (като чип карта или secure tokens);
- Нещо, което потребителят представлява (биометрична особеност – сканиране на отпечатък, ирис, ретина).

Чрез комбинация между тези три метода е възможно дейността на извършителите на нарушение да бъде затруднена или поне забавена.

Извършителите на този тип престъпление се отличават с арогантност, личностна несъстоятелност, висока готовност за агресивно отреагиране и манипулативно поведение.

В друга графа спадат кибертерористите и кибершпионите.

Най-общо определението на понятието „тероризъм", което можем да срещнем, е организането на криминална дейност със задължителна политическа цел, като се използват различни методи. За тази цел на извършителите им е нужно да имат достъп до парични средства, оръжия или взривни вещества, познания за използването им и добро укритие. Когато говорим за кибертероризъм, определението на понятието „тероризъм" не се променя изцяло, като изключение прави средата, която представлява киберпространство. От тази гледна точка на извършителите са им необходими персонални компютри и изградена връзка помежду им.

Необходимо е да се разграничат хактивизмът и кибертероризмът според съществената разлика в целта на злодеянието. В ситуация на кибертероризъм компютрите са оръжие или мишена на мотивирани интернационални или субнационални групи, които желаят да внесат страх сред околните.

Освен че нападат чуждите системи, кибертерористите се грижат за защитата на собствените си мрежи (например чрез криптиране) с цел да прикрият местонахождението си.

Характерни профилни характеристики на този тип извършители са завишеното ниво на готовност и необходимостта от адреналин. Личен мотив за тези нападения често е отмъщение за нанесени обиди или отказ от определена социална група.

Как можем да обясним и предвидим атаките в киберпространството? Хората знаят, че хакерството е сериозен проблем в нашето общество, но никой не е наистина наясно какви са причините, поради които хората хакват, какво ги кара да атакуват правителствени сайтове на други страни и как реагират, когато се чувстват заплашени от противник. Освен това няма конкретна рационална теория, която да обяснява хакерските дейности. Малко изследвания са проведени за справяне с този проблем. Само няколко проучвания са се опитали да разберат хакерите и кибертероризма по емпиричен начин поради трудността да получат данни от злонамерени потребители на киберпространството.

ВИДОВЕ КИБЕРАТАКИ

Компютърната престъпност е „специфично социално явление, статистически представено от съвкупността от различен вид и род престъпления с помощта на техническо средство – компютър, компютърни мрежи и продукти“. Терминът „киберпрестъпност“ обикновено се ограничава до описване на престъпна дейност, в която компютър или мрежа са съществена част. В по-разширен аспект този термин включва традиционни престъпления, в които се използват компютри или мрежи, за да се даде възможност за извършване на незаконни дейности. При това компютърът или мрежата може да бъдат както инструмент, така и обект на престъплението. Ето защо една от класификациите на компютърните престъпления ги разделя на две групи. В първата компютърът е средство за криминални дейности, като детска порнография, следене и тормоз, измама, пиратство и др. Във втората група компютърът представлява мишена или обект на криминални действия, състоящи се в кражба, вирусни атаки, зловреден код, промяна на данни и др.

Основните видове компютърни престъпления и атаки са: хакерски атаки, зловреден софтуер, кражба на финансови средства, кибершпионаж, киберследене и тормоз, кражба на интелектуална собственост, самоличност и данни, детска порнография (28).

С все по-голямото използване на компютърните технологии започва и разграничението на няколко основни групи и понятия. Най-често срещаните атаки са:

Зловреден софтуер

Зловреден софтуер е всеки софтуер, който е създаден с цел нанасяне на определени щети върху дадена компютърна система, като видовете му могат да варират от кражба на информация, през нейното модифициране до нейното цялостно разрушаване.

Съществуват множество зловредни софтуери, но един е нанесъл най-много щети, с което става и най-известен – Ransomware. Ransomware е вид зловреден софтуер, който блокира достъпа до данните на жертвата и заплашва да ги публикува или изтрие, ако не бъде платен откуп. Докато някои прости компютърни Ransomware могат да заключат системата по начин, който не е трудно да бъде пробит от опитен човек, по-напредналият зловреден софтуер използва техника,

наречена криптовирусно изнудване, която криптира файловете на жертвата по начин, който ги прави почти невъзможни за възстановяване без ключ за декриптиране.

Фишинг (phishing attack)

Това е най-разпространената практика за изпращане на имейли, чрез използване на известни източници като податели, с цел да се заблуди потребителят и да се получи чувствителна информация. В тези имейли се засягат теми, които са актуални за момента, като празници, събития с голяма популярност сред обществото, използват се дори теми за благотворителност, фалшиви имейли от техническа поддръжка, банки и т.н. Тези съобщения целят получаване на ценна информация https://krebsonsecurity.com/ главно относно кредитни/дебитни карти, също така и потребителски имена с цел злоупотреба и извличане на печалба. Подателите на този тип имейли се представят за легитимни източници (банки, ИТ съпорт и др.), като изискват от жертвата лични конфиденциални данни, свързани с номера на сметки, местоживеене, месторабота и пароли. Фишинг имейлите биват изпращани автоматично до многобройна група от потребители, докато съществуват и друг тип имейли – spear phishing, при които се набелязва конкретна жертва, която бива проучвана предварително.

Друга разновидност на фишинг измамите са фарминг имейлите, които представляват пренасочване на получателя/жертвата към друг сайт, без той да разбере. Ситуацията е следната: потребителят получава имейл с линк в него към напълно копиран сайт, като отново се изискват потребителски данни, които в случая се изпращат към злосторника, докато жертвата не разбира за фалшивия сайт.

Използване на чужда самоличност (представяне за друго лице с цел получаване на достъп до информация)

Този тип техника не е от най-трудните за изпълнение, тъй като не се изискват много действия от страна на нападателя, а само да бъде снабден с всички нужни идентификационни документи (например фалшив пропуск) и униформа, доближаваща се до официалната.

Кевин Митник, един от най-известните хакери през 90-те години, а сега работещ като консултант по IT сигурност, споделя, че социалното инженерство обикновено се основава на четири принципа:

1. „Всички искаме да помогнем“;

2. „Първичната ни реакция е да разчитаме на другия човек“;
3. „Не обичаме да казваме ‘не’“;
4. „Всеки обича да се похвали“.

Главните методи, които се използват за осъществяването на кибертероризъм или кибершпионаж, може да бъдат сведени до три – социален инженеринг (Social Engineering), груба сила (Brute Force attack) и техническо проникване в системите.

Атака тип налучкване (Brute Force)

Представлява опит за налучкване на данни за достъп. Това може да бъдат данни за достъп до хостинг акаунт, имейл акаунт, данни за достъп до администрацията на сайт и т.н.

Социално инженерство

Това е ползването на измама за заблуда на „жертви“, с чиято помощ извършителят осъществява дейността си. Социалното инженерство като тип кибератака не се основава на търсенето на пропуски в информационните системи, а на целенасоченото взаимодействие с най-слабото звено във веригата – човека (потребителя). Към социалното инженерство можем да прибавим и телефонната измама, тъй като при нея също има извличане на информация – чрез опит за влияние по телефона върху действията на „жертвата“. Като се прилагат техники като телефонен spoofing – ситуация, при която се фалшифицират данни, в този контекст се подменят телефонни номера.

DdoS атака

Атаките DdoS (Distributed denial-of-Service) имат за цел да спрат достъпа на потребители до важна информация или до определени сайтове. Този вид атаки са лесни за изпълнение, което ги превръща в често използвани от злонамерени хакери. При атаката DdoS атакуващият задава команда към предварително подготвена бот мрежа да атакуват. Ботмрежата (bot-net) представлява десетки ботове (зловреден софтуер, като операционни системи или програми върху компрометирани машини). Ботовете заливат жертвата с трафик или информация, докато услугата спре да работи и стане недостъпна.

Атаката DdoS действа по два начина:

• Изчерпване на пропускателната способност на канала за връзка с интернет;

• Изчерпване на изчислителните ресурси на сървъра (памет, процесорно време, дисково пространство).

Най-честите жертви на атаките DdoS са:

• Онлайн магазини;

• Сайтове, асоциирани с правителствени организации;

• Сайтове на политически партии;

• Сайтове с онлайн плащания;

• Сайтове за онлайн игри, залагания и др.;

• Сайтове на финансови организации, банки, кредитни институции;

• Медийни и новинарски сайтове и др.

Последиците от една атака *DdoS* може да са:

• Финансови загуби и източване на парични средства;

• Накърняване на репутацията;

• Спад на доверието на клиентите и загуба на клиенти;

• Кражба на конфиденциална информация и правни последици;

• Спад на продажбите и пропуснати ползи;

• Необходимост от мерки за намаляване на щетите и възстановяване на информацията, репутацията и доверието на клиентите.

Проникване в средата

Този тип атака се реализира, когато хакерът е способен да чете и видоизменя различни съобщения по собствена воля, като присъствието му е незабелязано.

Атаката „човек в средата“ е атака, при която хакерът може да следи комуникацията „потребител – уеб сървър“. По този начин е възможно да се засекат както потребителски имена и пароли, така и друго съдържание, излизащо от или отиващо към потребителя. Сред протоколите, които пренасят съдържание, включително пароли, в незащитен вид, са HTTP, IMAP, POP3, TELNET, FTTP, SMTP. В такива случаи и защитната стена не предоставя желаната сигурност, защото тя пази от външни заплахи, а тази е вътрешна.

Защитата от „човека в средата“ обаче е сравнително проста – разделяне на мрежите и избягване на некриптирани протоколи. Без тези мерки паролите губят значението си, колкото и да са сложни, подчертава експертът по информационна сигурност Мауро Израел.

СПОСОБИ, ТЕХНИКИ И ИНСТРУМЕНТАРИУМ ЗА ПРОТИВОДЕЙСТВИЕ НА КИБЕРАТАКИТЕ

Неетичното хакерство е законово престъпление, но това не спира хакерите да разкриват чужда лична информация и да я използват за собствена изгода. За тази цел злонамерените хакери използват набор от инструменти, трикове и способи.

Нападетелите, използващи социалното инженерство като атака, също разполагат с различни инструменти. Събирането на информация е една от най-важните задачи на социалния инженер, за да свърши ефективна работа, затова атакуващият съчетава различни информационни технологии с физически (материални) инструменти.

Пример за такъв софтуер с отворен код е Maltego, използван за разузнаване и събиране на информация, като интерфейсът му представя тази информация по лесен и удобен за разбиране начин. Maltego позволява да се идентифицират ключови връзки между разглежданите обекти и да се намерят нови, непознати взаимоотношения между тях. Maltego реализира автоматично множество връзки между разглеждания обект и всичко около него, като спестява часове търсене на този тип информация. Пример за прилагане на програмата е въвеждането на имейл адреса на „жертвата“, а след това програмата автоматично показва регистрация на имейл адреса в множество сайтове за автомобили, което дава съществена насока на нападателя за обекта на атаката. Инструментите невинаги са под формата на софтуер, като за същата цел може да бъдат използвани и най-обикновените телефони. Използването на телефоните като инструмент за социална инженерна атака е често срещано явление както в бизнес средите, така и при малките мишени. В тази ситуация се използват предплатени карти, ваучери, т.нар. „burn phones“, чиито номера не може да бъдат проследени. Примери за подмяна на телефонния номер са:

- Подмяна с телефонен номер на известна куриерска фирма, национална пощенска служба;
- Подмяна с телефонен номер от коорпоративната ви група;
- Подмяна с телефонен номер на интернет доставчик.

Физическите мерки за сигурност не включват компютъра като средство за осигуряване на защита. По-често такива са ключалки, камери, датчици за движение, сензори и т.н. – това са обектите,

въху които добрият социален инженер работи за разбиране на техния начин на работа.

Примери за такива устройства са:

• Камерите, които са добър помощник на злосторника, тъй като са удобни за бързо заснемане на информация и са налични в различни незабележими форми и размери;

• GPS проследяващите устройства, които се прикачват към обекта на проследяване (кола, велосипед и др.) и дават точното му местоположение. Тези уреди са леки и лесни за скриване, като сами се задействат и изключват при наличието на вибрации;

• Ключалки – разбиването на ключалки не е отживелица, тъй като това умение осигурява лесен достъп до ценна информация;

• Записващи/подслушвателни устройства – тези устройства съществуват във всякакъв вид и форма (най-позната е химикалката), отново са трудни за разкриване и ефективно събират нужната информация.

Инструменти за проникващи (penetration) тестове

Този тип инструменти се използват за тестове за информационна сигурност на мрежи, уеб приложения и services – със и без предварително предоставен достъп. Тестовете за проникване са най-честата форма на решение за киберсигурност, целящо да оцени сигурността на системата. Според IRRA solutions проникващият тест е реалната, практическа гледна точка на външно лице, което се опитва да заобиколи мерките за информационна сигурност, прилагани в дадена организация, с цел установяване на уязвимости в информационната среда. Тези уязвимости може да бъдат от всякакво естество – от физическото разположение, или архитектурата на информационната инфраструктура, през конфигурацията на различните информационни активи (сървъри, мрежови устройства, потребителски станции), до различни слабости в приложенията/програмите, които се използват в организацията.

SN1PER е пример за инструмент за уеб сканиране на уязвимости. Инструментът е особено добър в изброяването и сканирането на известни уязвимости.

Инструменти за разбиване на пароли

Разбиването на пароли е процес на разкриване на пароли от данни, които са били съхранени или предадени от компютърна система. Общият подход (атака с груба сила) е многократни опити да се отгатне паролата и проверяване на наличен криптографски хеш на паролата. Целта на разбиването на пароли може да бъде: помощ на потребителя да възстанови забравената си парола, получаване на неоторизиран достъп до системата или превантивна мярка от системните администратори да проверяват за лесно разбиваеми пароли.

Пример за такъв инструмент е JOHN THE RIPPER, който оглавява и класациите в областта на инструментите за пробив. Този хакерски софтуер е предназначен да разбие дори много сложни пароли.

След запознаването с множеството вариации на инструменти за нарушаване на потребителската защита става ясно, че инвестирането в информационни технологии не е най-ефективният метод за защита от атаки. Развиването на умения за разбиране и идентифициране на основните понятия, запознаване с видовете атаки и инструментите за тях е един от начините за създаване на добри практики за ИТ сигурност за потребителя и като цяло за организацията.

Формална уязвимост – човешки фактор

Човешкият фактор като компонент на дадена информационна среда в контекста на киберсигурността се изразява както в интеракциите между отделните потребители на киберпространството, така и в „срещата“ им с различни технологични способи. В книгата си „Информационна среда за трансфер на технологии“ Стоян Денчев дефинира *информационната среда* като **„съвкупност от информационни фондове, информационни технологии и интеракциите между хората и оборудването, осигуряващи социалната инфрастуктура за общественополезна реализация на един или друг специфичен информационен процес в рамките на определена предметна област“**. Резултатите от тези интеракции са интерактивни процеси, които имат не само технически, но и социален характер. Ако техническите са пряко свързани с дадени информационни технологии и ресурси, то социалните представляват явление, отразяващо нивото на развитие на интелектуалните

способности, социалната ангажираност и култура на отделния индивид и обществото като цяло.

Макар че повечето престъпления в киберпространството са целенасочени, често се извършват и случайно. Кликването върху уж безвреден линк в имейл от приятел или просто лошата дисциплина и използването на слаба парола могат да отворят врати за киберпрестъпниците и техните сътрудници. Част от проблема произтича от това, което бившият специален агент на ФБР Джон Янарели нарича „умора от нарушения", и от общото, често срещано разбиране, че киберпрестъпността е „отговорност на някого другиго". Янарели, който сега работи като консултант по киберсигурност, заявява, че готовността на банките и компаниите за кредитни карти за ограничаване на загубите на потребителите, засегнати от измами, създава фалшиво чувство за сигурност. Тази „умора от нарушения" се изразява в това, че потребителите достигат точка, в която намират все по-малко изненадващ пробива в сигурността на данните.

Според Джулиан Асандж (основател на Wikileaks): ,,Не на последно място стои човешкият фактор, т.е. професионализмът и етичността на работещите. Каквито и системи за сигурност да бъдат прилагани, в крайна сметка остава човешкият фактор".

Прилагането на технически способ като самостоятелно и единствено решение е слабо ефективно в предотвратяването на нарушаване на сигурността. Организациите трябва да създават и поддържат култура в среда с познавателен характер относно реалните заплахи за информационната сигурност. Служителите трябва да бъдат обучавани за важността от информираност относно сигурността, включително да получават поведенческа подготовка.

„За повечето компании най-добрата защита е обучението на служителите да разпознават киберзаплахите – казва Янарели. – Хората трябва да се научат да разпознават атаки като фишинга, китолова и социалното инженерство, с които киберпрестъпниците се опитват да получат поверителна информация, например пароли, като се представят за приятели или колеги."

За въвеждането на информационната сигурност като практика на всяко ниво от организацията, са нужни постоянно наблюдаване и подобряване, изграждане на практики на служителите и намаляване на риска от човешка грешка.

Необходимостта от обучение на персонала по въпросите на

киберсигурността остава неоспорим факт. Във връзка с това наличието на различни нива на обучение и свързани с тях обучителни подходи и методи само може да стимулира креативността на обучителите. Описаните нива за обучение на персонала по проблемите на киберсигурността не се разглеждат в противопоставяне, като по-добри или по-лоши. С тях просто се разкриват алтернативни възможности, изборът сред които се базира на фактори като ниво на амбиция при изграждането на състояние на киберсигурност, способности на лицата, планиращи и провеждащи обучението, апетит към рисковете за киберсигурността на организацията и т.н.

Инвестирането в продукти за информационна сигурност не може да гарантира пълна защита, ако не бъде придружено от правилни ИТ умения за сигурност и добро разбиране на киберзаплахите. Само чрез разбирането и идентифицирането на основните понятия, залегнали в безопасното използване на ИКТ, е възможна защитата на системите и на информацията в тях. Един от начините за създаване на добри практики за ИТ сигурност за потребителя и понататък – за организацията, е чрез прилагане на признати програми за обучение и сертифициране, които сравняват потребителските нива на умения и знания с международно признат стандарт.

В контекста на киберсигурността терминът „човешки фактор“ се отнася до ролята, която потребителите играят в процеса на сигурността. Потребителите имат определени разбирания, които могат да повлияят положително или отрицателно на процеса на сигурност. Проучване, проведено от Ругхинис и Рюнис в Европейския съюз, очертава три вида крайни потребители, които отчитат лошо поведение в киберпространството:

- Когнитивно мързеливи потребители;
- Икономически рационални потребители;
- Социални потребители.

Мързеливият тип потребители обикновено не са достатъчно информирани, те са склонни да предпочетат комфорта дори ако сигурността е изложена на риск. Икономически рационалните потребители избират да балансират разходите си и в резултат на това имат ниско ниво на съответствие с изискванията за сигурност. И накрая, социалните потребители просто се интересуват от желаната онлайн услуга и вярват на доставчика на услуги за всички въпроси, свързани със сигурността. Тези потребители са

идеалната плячка за социалноинженерни измами.

Общото между всички тези потребители е минималното съответствие на мерките за киберсигурност. Освен това Пфлигър и Капуто изказват предположение, че като цяло сред много потребители съществува схващане, че мерките за сигурност са пречка и вследствие на това загуба на време; следователно мерките за сигурност се игнорират. Например, ако потребителят възприема уведомленията за промяна на паролата като досадни, той е склонен да ги пренебрегне. От друга страна, това устойчиво поведение компрометира ефективността на мерките за сигурност.

Според доклада на Политехническия институт във Вирджиния – „Вирджиния Тех", това възприятие на потребителя може да бъде приписано на трудността да се възприеме важността на сигурността, включително очевидното недоверие към и неправилното тълкуване на мерките за сигурност. Томсън и др. предполагат, че липсата на информираност в организациите също допринася за несигурното поведение сред потребителите (39).

За съжаление, такива погрешни възприятия и лошо поведение и култура, независимо дали на работното място, или у дома, не само правят съответния потребител мишена за атака, но и излагат на риск други потребители.

Изграждането на култура за киберсигурност е от решаващо значение за промяната на поведението на потребителите и създаването на „естествено поведение", което се придържа към определени мерки за сигурност. Това се оценява на национално равнище в редица държави. По-специално Южна Африка (SA) има за цел да развие култура на киберсигурност. Това е в съответствие с опитите и стремежите на редица развити държави, като САЩ, Обединеното кралство и Канада (Белият дом, 2009 г.; Кабинетът на правителството на Канада, 2010 г.).

По-голямата част от случаите на инсталиране на зловреден софтуер се дължат на действията на потребителите, които посещават уеб страници със съмнително съдържание, отварят имейли и свалят файлове от неизвестни податели или инсталират нелегитимни приложения (26).

Според Шари Пфлигър киберсигурността е предотвратяване и защита от кибератаки както чрез технология, така и чрез подход, ориентиран към човека. Въпреки това дълго време технологично

ориентирани решения, като антивирусен софтуер, криптиране и защитни стени, са били използвани като самостоятелно средство за защита. Докато продължава да се възприема, че самостоятелното им прилагане е достатъчно и правилно, такива решения няма да са достатъчни за намаляване на рисковете за киберсигурността. Една от причините за това е, че много потребители възприемат тези мерки за сигурност като пречка или се поддават на митовете и заблудите за киберсигурността. Това възприятие на потребителите често се дължи на трудността на мярката за сигурност и/или на недоверието в нея и неправилното ѝ тълкуване. Освен това в проучване, което изследва потребителската устойчивост, се показва, че при препоръка към потребителите да променят паролите си, поканата е била пренебрегната или забавена, тъй като потребителите възприемат тази мярка за сигурност като загуба на време. Потребителите често не познават рисковете за киберсигурността, което ги прави лесни мишени за експлоатация. Освен това хората се смятат за заплаха не само за себе си, но и за другите, дори за националната сигурност като цяло. Поради споменатите по-горе наблюдения относно човешкия фактор налагането на по-човешки ориентиран подход (т.е. култура на киберсигурността) към киберсигурността е задължително. Ван Никерк и Фон Солмс възприемат създаването на такава култура като „ключ към управлението на човешкия фактор“. Обаче това, което липсва в момента, е добре дефинирано и очертано определение на културната сфера на киберсигурността. Поради това една от подцелите на този труд е да предложи определение на явлението култура на киберсигурността.

Международният съюз по телекомуникации (ITU) разглежда изграждането на култура на киберсигурността като основен подход към сигурността в киберпространството. Осъзнавайки това, много развити държави, като САЩ, Великобритания и Канада, се стремят да развият такава култура сред своите граждани. В частност Южна Африка очерта създаването на култура на киберсигурността като основна цел в своята проектна рамка на политиката в областта на киберсигурността.

Според Соланж Гернаути, професор от университета на Лозана (UNIL) и международен експерт по киберсигурност и киберотбрана, един от стълбовете на тази култура на киберсигурност са осведомеността и образованието. Установено е обаче, че дори потреби-

телите, които притежават повече знания за киберсигурността, не действат непременно по различен начин от тези, които нямат никаква подготовка по отношение на киберсигурността. Независимо от факта, че нивото на информираност на потребителя оказва положително влияние върху поведението му, все още съществува явна пропаст между нивата на осведоменост на потребителите и съответните практики и поведение.

Важно е да се отбележи, че потребителите на информационната среда трябва да притежават добра подготовка и култура, за да могат да вземат дейно участие в целия цикъл на информацията.

ПОЛИТИКИ, СТАНДАРТИ И НАСОКИ ЗА ПОВИШАВАНЕ НА КИБЕРСИГУРНОСТТА

Една от основните причини за създаването и налагането на политика на сигурността е да се гарантира, че инвестираните ресурси за създаване на сигурност на информацията не са вложени напразно. От друга страна, без утвърдени правила за Контрола на достъпа до информация, Управлението на комуникациите и операциите, Човешките ресурси и т.н. няма да съществува сигурност на познатите ни вече стълбове, а оттам – и на информацията като цяло.

След 25 май 2018 г. политиките, стандартите и насоките за информационна сигурност (включително киберсигурността) не са чак толкова непознати явления за всички потребители на онлайн пространството. Именно на 25 май 2018 г. влязоха в сила санкциите, свързани с въвеждането на ОРЗД/GDPR (Общ регламент за защита на личните данни/General data protection regulation), който е в сила на територията на целия Европейски съюз. Въвеждането на GDPR е една от най-важните реформи в ЕС и основната му цел е да изгради по-голям контрол върху персоналната информация, като предостави единен подход за неприкосновеност на данните. След въвеждането на санкции за неспазването на Регламента необходимостта от актуализация на политиката за сигурност набра такава популярност, че някои сайтове дори предлагат безплатни шаблони за изготвяне и прилагане на политика за информационна сигурност. В такива сайтове намираме и разграничението между политика, стандарт и насоки за информационна сигурност:

➢ ***Политиката*** обикновено е документ, очертаващ конкретни изисквания или правила, които трябва да бъдат изпълнени. В областта на сигурността на информационната или мрежовата политика те обикновено са тясно специфични и обхващат една област. Например политиката за ползване ще покрие нормите и правилата за правилната употреба на компютърните съоръжения. Обикновено политиката е кратка и стройна стратегия, в която организацията дефинира и разписва правилата за защита на информационните си ресурси при възникването на заплахи и инциденти, застрашаващи сигурността им. Политиката, както и информацията, подлежи на промяна. Тъй като информацията е подвижна, развива се, а заедно с нея се променя инфраструктурата, възникват нови заплахи. Промяната в обществените отношения и общоприетите стандарти обикновено води до необходимостта от изменение на политиката. Политиката трябва да описва възможностите за усъвършенстването на управлението на информационната сигурност в отговор на промените (стратегията, бизнес условията, човешките ресурси, работните процеси, активите и т.н.), влиянието на външните фактори и новопоявили се или изменени заплахи и уязвимости.

Политиките определят задължителни насоки, които влияят върху благоприятното организационно поведение при използването на системи или работа с данни (36). Всички политики за информационна сигурност трябва да отговарят на целите на организацията и да ги подчертават (37). Като се има това предвид, политиките за сигурност се създават, за да съобщават протоколи за сигурност, да дават ясни роли и отговорности и да осигуряват на служителите насоки за приемливо използване, за да се гарантира поведение на сигурност по време на изпълнението на работни задачи. Ролите, отговорностите и насоките също дават яснота за това кой трябва да се свързва и как се обработват инциденти с информационната сигурност. Когато политиките са сложни, двусмислени, неясни или трудно разбираеми за потребителите, отношението към спазването на правилата е негативно. Организациите трябва да направят своите политики възможно най-разбираеми, подходящи и достъпни за всички служители.

Политиката за сигурност трябва да изпълнява много цели:

- Да защитава хора и информация;

• Да определя правилата за предвиденото поведение на потребителите, системните администратори, мениджърите и персонала по сигурността;

• Да упълномощава персонала по сигурността да следи, проучва и разследва;

• Да определя и разрешава последиците от нарушения;

• Да определя основната позиция на компанията по отношение на сигурността;

• Да намалява риска;

• Да наблюдава за спазването на правилата и законодателството.

Политиката на информационна сигурност осигурява рамка за най-добри практики, които може да бъдат следвани от всички служители или потребители. Тя помага да се гарантира, че рискът е сведен до минимум и че на всеки инцидент по сигурността е ефективно отреагирано. Политиката на информационна сигурност също така помагат на служителите и потребителите да се превърнат в участници в усилията на компанията/организацията да подсигури информационните си активи, а процесът на разработване на тези политики ще помогне да се определят информационните активи. Политиката на информационна сигурност определя отношението на организацията към информацията и обявява вътрешно и външно, че информацията е актив, собственост на организацията, и трябва да бъде защитена от неразрешен достъп, промяна, разкриване и унищожаване.

Политиката на информационна сигурност може да се раздели на няколко типа, като се разгледа нейният обхват: обща (включва например приемлива политика за шифриране, политика за отговор при нарушаване на данните, правила за електронна поща, етична политика), мрежова защита (включва например политика за оценка на придобиването, политика за отдалечен достъп, правила за инструменти за отдалечен достъп и др.), защита на сървъра (включва например лабораторна политика за сигурност, правила за сигурност на сървъра и др.), защита на приложения и т.н.

➢ ***Стандартът*** обикновено е съвкупност от специфични за системата или процедурно специфични изисквания, които трябва да бъдат изпълнени от всички (40). Стандартът за сигурност е като всеки друг стандарт в която и да е друга индустрия. Стандартът е оповестена спецификация, която установява общ език

и съдържа техническа спецификация или други точни критерии, като е разработена така, че да се използва последователно, като правило, насока или определение. Освен това според ISO стандартите допринасят за опростяването на живота и повишават надеждността и ефективността на стоките и услугите, които използваме. По същество стандартът е общ набор от правила, определения и договорени „регламенти“, на които всички страни могат да се позовават за обща справка. Стандартът е набор от минимални изисквания, които дадена организация трябва да изпълни, за да претендира, че отговаря на стандарта.

Международната организация по стандартизация (ISO) определя стандарта като *„документ, създаден с консенсус и одобрение на признат орган, който го предоставя за обща и многократна употреба, правила, насоки или характеристики на дейностите или техните резултати, насочени към постигане на оптимална степен на ред в даден контекст“*. Разработени са много стандарти за киберсигурност, за да се помогне на организациите да управляват по-добре рисковете за сигурността, да осъществят контрол за сигурност, отговаряйки на законовите и регулаторните изисквания, също така да се постигнат високи резултати и ползи при разходите.

Стандартите за киберсигурност се размножават, правителствата и предприятията все повече налагат изпълнението им. Повече производители и продавачи изграждат и продават продукти и услуги в съответствие на стандартите. Освен това все повече организации се включват в разработването на стандарти. Стандартите за киберсигурност се възприемат, защото са полезни, те осигуряват осезаеми ползи, които оправдават времето и финансовите ресурси, необходими за изготвянето и прилагането им. Технологиите за сигурност не са в крак с бързото развитие на информационните технологии, оставяйки системите, данните и потребителите уязвими както за общоприетите, така и за иновативните заплахи за сигурността. Политически мотивирани противници, финансово мотивирани престъпници, злонамерени нападатели и злоумишлени или невнимателни упълномощени потребители са сред заплахите за системите и технологиите, които могат да застрашат киберсигурността, икономическата сигурност на всяка страна, идентичността на потребителите, неприкосновеността на личния живот и

общественото здраве и безопасност. Макар да е невъзможно премахването на всички заплахи, подобренията в киберсигурността могат да помогнат за управлението на рисковете за сигурността, като затруднят атаките и намалят ефекта им.

Стандартите за киберсигурност осигуряват и други предимства. Тъй като стандартите като цяло включват най-добрите практики и изисквания за съответствие, тяхното използване обикновено води до подобряване на качеството. Стандартите намаляват броя на техническите отклонения и позволяват на потребителите лесен достъп до взаимозаменяеми технологии. Програмите за спазване на стандартите предлагат начин за измерване на продуктите и услугите в съответствие с обективни критерии и осигуряват основа за сравнение на продуктите, като например потвърждаване, че те предлагат определени групи защитни елементи. Потребителите често се възползват от икономиите на разходи, които произтичат от разработването, производството, продажбата и доставката на стандартизирани, оперативно съвместими продукти и услуги.

Друго предимство на стандартите за киберсигурност е, че процесът на разработване на стандарти, със своите типични практики за привличане на широк спектър от експерти по въпросите, създаване на прототипи и включване на критерии и методологии за оценка на съответствието, спомага да се гарантира, че стандартите са приложими и отразяват препоръчителните практики. Продукти или услуги, за които е доказано, че отговарят на стандартите за ИТ сигурност, може да се очаква да предлагат по-голяма увереност от нестандартните продукти.

- ***Насоките*** обикновено са сбор от специфични за системата или „процедурни“ предложения за най-добра практика. Те не са изисквания, които трябва да бъдат изпълнени, но са силно препоръчани. Ефективните политики за сигурност често правят препратки към съществуващи стандарти и насоки за информационна сигурност.

Изследването на Хасингер и Кранз показва, че създаването и популяризирането на информационните политики за сигурност са основополагащ елемент на всяка програма за управление на информационната сигурност и оказват положително влияние върху информираността на служителите. Изследвания от Сафа също отбелязват, че политиката на информационна сигурност на органи-

зацията оказва огромно влияние върху поведението, свързано с грижата за сигурността.

В книгата си „Информационни системи в управлението“ д-р Пенчо Пенчев отбелязва основните изисквания към информационните системи за управление, които по характеристики би могло да се отнесат към човешката система при ежедневни процеси в киберпространството. От техническа гледна точка управленската информационна система се състои от компютърни мрежи, програмни продукти, бази данни, технически и програмни средства. Подобни системи са насочени към постигането на множество цели, основната от които е „производство“ на информация, необходима при изработването на управленски решения. Подобно на нея човешката система се състои от сходни способи за постигане на дадени цели (например: процесор – мозък, памет – компютърна памет, и т.н.). Човешкото тяло, както и компютърът, съдържат мрежа от милиарди невронни сигнал-процесори. Основната част от тях е в мозъка, чиято химико-електрическа активност се захранва от периферната нервна система.

Част от особеностите и изискванията към тези системи са следните:

- Системата трябва да решава нови задачи. Още при проектирането е необходимо да се предвиди възможност за въвеждане на нови задачи. Това повишава ефективността на системата. Както в човешкото ни ежедневие, всеки се сблъсква с нови задачи и предизвикателства и е нужно да е подготвен за такива ситуации;
- Системата трябва да бъде съобразена изцяло с вижданията на висшето ръководство. На базата на пълномощията оттам се определят приоритетните направления, необходимите ресурси, на разработчиците се предоставя необходимата информация и пр. Потребителите също е важно да имат определени приоритети, тъй като впоследствие това определя тяхното адекватно присъствие в киберпространтството;
- Системата осигурява типовост на проектните решения. Това гарантира, че ще обхваща с проектни решения възможно повече потребители;
- Системата постоянно се усъвършенства и се развива, бързо реагира на възникващите нови задачи в управлението, осигурява възможност за усъвършенстване на вече решени задачи. По същия

начин човекът трябва да развива своите познания и начина на пребиваването си в киберпространството, било то поради наличието на нов тип заплаха или риск;

• Системата трябва да е разработена по такъв начин, че да може да си взаимодейства и да е съвместима с други системи в съответствие с установените правила;

• Многобройните управленски задачи може да се решават чрез използването на единна информационна база. В своята работа организациите все по-често започват да **зависят** от информационните технологии. Те очакват, че именно информационните системи в управлението не само ще поддържат равновесното им състояние, но и ще им предоставят нови възможности за реализация на ежедневните задължения и крайни цели.

Необходимо е да знаем и да разбираме начина на работа на информационните системи за управление, тъй като това ще ни бъде от полза и наше улеснение при изпълнението на всякакъв вид електронни услуги или заявки.

СТРАТЕГИИ И МЕРКИ ЗА КИБЕРСИГУРНОСТ ПРИ ЕЛЕКТРОННО УПРАВЛЕНИЕ

За да открием, спрем или избегнем кибератака в ежедневен процес при използване на електронни услуги на електронно управление, ни е необходимо не само техническо разглеждане на проблема. Необходими са ни закони и подзаконови актове, които да спомогнат за намаляването на компютърните престъпления. Трябва по-добре да разберем формите и причините на злонамерените действия в киберпространството, ефективността на мерките, включително в областта на правоприлагането, за да видим какви са механизмите за въздействие и прилагане на мерки за сигурност, кога и къде се налага регулиране.

През 2013 г. Luiijf, Basseling и Graaf проучват и сравняват деветнадесет национални стратегии (Австралия, Канада, Чехия, Естония, Франция, Германия, Индия, Япония, Литва, Люксембург, Румъния, Холандия, Нова Зеландия, Южна Африка, Испания, Уганда, Великобритания (2009 и 2011) и САЩ) за киберсигурност от осемнадесет различни държави по целия свят. Техният доклад разкрива различията и сходствата, открити в начина, по който народите се

отнасят към киберсигурността. На базата на анализа се изготвя списък с препоръки за подпомагане на други страни в разработването на национални стратегии за киберсигурност[30]. Наред с други неща, които може да бъдат извлечени от анализа, факт е, че само три национални стратегии – на Уганда, Южна Африка и Румъния, изрично посочват създаването на култура на киберсигурността като стратегическа цел.[31]

След 2013 г. част от стратегиите на разгледаните държави търпят промени с цел подобрение:

Австралия

Последната версия на националната стратегия за киберсигурност на Австралия (2017 г.) обръща внимание именно на културната промяна, заявявайки нейната по-голяма важност от тази на техническите решения за смекчаване на проявите на киберопасност. В предисловието на министър-председателя на Австралия Малкълм Търнбул присъства изявление за това, че стратегията има за цел да насърчи подобрената институционална култура на киберсигурност и да повиши информираността за киберпрактиката в правителството и бизнеса, за да може всички австралийци да бъдат сигурни онлайн. Той отбелязва също пропуските в нацията: „Много австралийци и организации също просто не са наясно с рисковете, пред които са изправени в киберпространството. Повечето от нас заключват вратите и се грижат за вещите си, но не предприемат същите мерки спрямо своите устройства и онлайн информация. Правителството се ангажира да оборудва австралийците с правилните умения за киберсигурност и да повиши информираността им за киберсигурността, така че всички да могат да се възползват от възможностите в киберпространството“.[32]

Според новия доклад от проучването на Организацията на обединените нации за електронно правителство, 2018 г., Австралия е в топ 10 на страните с развито е-правителство – на трето място с

[30] **Luiijf**, E., K. **Besseling**, P. **De Graaf**. Nineteenth national cybersecurity strategies. – In: *Int. J. Crit. Infrastructures*, vol. 9, no. 1 – 2, pp. 3 – 31, 2013.

[31] **Gcaza1**, N., R. **von Solms**. Cybersecurity Culture: An ill-defined Problem.

[32] Australia's Cyber Security Strategy 2017.

индекс 0.9053.[33] Сайтът на астралийското е-правителство разполага с раздел „Киберсигурност за информация“ с препратка за потребителите към Австралийския център за киберсигурност.

Канада

Ситуацията в Канада също се е променила – освен стратегията за киберсигурност от 2010 г. държавата разполага с нова такава, публикувана през юни 2018 г. Първата версия на стратегията е изградена върху три стълба:

- Осигуряване на правителствени системи;
- Партньорство за осигуряване на жизненоважни киберсистеми извън федералното правителство;
- Помощ за канадците да бъдат сигурни онлайн.

Първият стълб има за цел да установи ясни роли и отговорности, да засили сигурността на федералните киберсистеми и да повиши осведомеността за киберсигурност в цялото правителство.

Вторият стълб обхваща редица партньорски инициативи с провинциите и териториите и включва частния сектор и секторите с критична инфраструктура.

Третият стълб обхваща борбата с киберпрестъпността и защитата на канадските граждани в онлайн среда. Загрижеността за поверителността се разглежда по-специално в този трети стълб. При тази версия на канадската стратегия за киберсигурност от 2010 г., в 17-те ѝ страници, за култура на киберсигурността се споменава единствено в края на документа: *„Крайната цел на правителството е да се създаде култура на кибербезопасност, при която канадците да са наясно както със заплахите, така и с мерките, които могат да предприемат, за да осигурят безопасното използване на киберпространството. Създаването на такова съзнание изисква продължителни усилия в продължение на няколко години“*.[34] Но в стратегията от 2018 г. още във въведението забелязваме нещо много важно за всеки потребител: ***„Киберсигурността някога беше в областта на техническите експерти, но сега, в нашия диги-***

[33] UNITED NATIONS E-GOVERNMENT SURVEY 2018 Department of Economic and Social Affairs GEARING E-GOVERNMENT TO SUPPORT TRANSFORMATION TOWARDS SUSTAINABLE AND RESILIENT SOCIETIES.

[34] Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada.

тален свят, ние всички играем роля в нашата индивидуална и колективна киберсигурност"[35]. Това изречение подчертава необходимостта от култура на киберсигурност у всеки, не изисквайки от никого високи технически и/или технологични познания, което съвпада с възгледите на мнозинството специалисти в тази област, че всеки, независимо от техническата си подготовка, трябва да развива собствената си култура на киберсигурност, защото присъствието му онлайн е неизбежно и никак не е безопасно. В сайта на правителството на Канада също присъства секция „Киберзащита", където гражданите могат да научат за потенциалните рискове от онлайн дейностите и как да останат в безопасност, когато са свързани.

Чехия

Чешката република до момента разполага с две стретегии за киберсигурност, първата – за периода 2012 – 2015 г., а втората – за периода 2015 – 2020 г. Първата е съвсем кратка и дори не предлага дефиниция за киберсигурност, която за разлика от това присъства във втората стратегия за киберсигурност на Чехия. Основните цели на стратегията за киберсигурност включват защита срещу заплахи, на които са изложени информационните и комуникационните системи и технологии, и смекчаване на потенциалните последствия в случай на атака срещу ИКТ. Стратегията се фокусира главно върху безпрепятствения достъп до услуги, целостта на данните и поверителността на киберпространството на Чешката република и е координирана с други свързани стратегии и концепции. Последващата я стратегия се опира на четири принципа:

- Защита на основните човешки права и свободи и на демократичните принципи;
- Цялостен подход към киберсигурността, основан на принципите на субсидиарност и сътрудничество;
- Изграждане на доверие и сътрудничество между публичния и частния сектор и гражданското общество;
- Изграждане на капацитет за киберсигурност.[36]

---

[35] National Cyber Security Strategy Canada's Vision for Security and Prosperity in the Digital Age 2018.

[36] Czech Republic – National Cyber Security Strategy 2015 – 2020.

Част от целите, които са си поставили в стратегията, е *Образование, повишаване на осведомеността и развитие на информационното общество*, като се засягат най-вече промени в учебни планове и обучение на служители от публичния сектор.

Въз основа на главните цели на Стратегията и в координация с всички заинтересовани страни е изготвен План за действие за определяне на конкретни стъпки, отговорности и срокове за тяхното изпълнение и одит. Специализиран отдел непрекъснато наблюдава, обсъжда и оценява в сътрудничество с други заинтересовани страни нивата на постигане на индивидуалните цели. Представя се годишен „Доклад за състоянието на киберсигурността в Чешката република", към който се прилага информация за изпълнението на плана за действие. Докладът информира правителството и широката общественост за ефективността на приетите мерки и за напредъка по изпълнението на задачите, определени в стратегията.[37]

През септември 2016 г. чешкото правителство стартира инициатива 202020, която да помогне на Чешката република да навакса сред държавите членки на ЕС, водещи в областта на електронното правителство. Проектът популяризира настоящите услуги за електронно правителство, обяснява как работят, и подчертава допълнителния напредък.[38] Една от причините, поради които е стартирана инициативата, е резултатът от световното проучване на ООН за електронно правителство на държавите членки. От този доклад се определя нивото като решаващо за устойчивото развитие и просперитета на държавите членки. От 2016 г. Чехия е слязла в класацията от завидното 50-о място с 4 позиции надолу. В класацията преди Чехия са били държави като Беларус, Чили, Казахстан, Барбадос, Бразилия и България. Съседната им Словакия, от друга страна, се изкачва с 18 позиции на 49-о място през същите две години. През 2001 г. Чехия бе класирана на 30-о място в класацията на Световните лидери. През 2008 г. Чешката република бе на 25-о място и имаше амбицията да бъде сред първите десет. През 2010 г. все още поддържа 33-та позиция в световен мащаб. През тези годи-

[37] Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.

[38] http://202020.cz/category/clanek/

ни Чехия е в първите категории страни – с много висок индекс на развитие на електронното правителство (EGDI), заедно с Кипър, Русия и съседните Полша, Германия и Австрия. Но докато светът продължава да развива своето електронно правителство и онлайн услуги, Чешката република сякаш спира. През 2012 г. слиза до 46-о място, две години по-късно дори до 53-то място.[39]

Чехите говорят за положението в страната си. „В продължение на две години ние се опитваме да убедим политическото представителство на държавата, че сегашното състояние на развитието на електронното правителство в Чешката република е неустойчиво. Истината е, че от създаването на основни регистри, чешки точки за достъп до данни развитието на електронното правителство е спряло в нашата страна. Постепенно попадаме в електронната праистория“, коментира Зденек Зайечек, председател на Съюза на ИКТ, коментирайки слабите резултати на Чешката република в рамките на Организацията на обединените нации. Следващият доклад на ООН е след две години, а Чехия работи усилено върху това да направи своя голям скок и да успее да се издигне в класацията. За тях важните стъпки за този успех се състоят първо в законодателството, след това да се разгледат предимствата на онлайн услугите на електронното правителство и не на последно място, как потребителите ще използват тези услуги.

От всички тези усилия на Чехия личи, че концентрира усилията си повече върху цялостно изкачване в световната класация за развитие на дигиталната мощ и подготовка. Според мен трябва да насочат усилията си повече към подготовката на крайния си потребител и неговите необходимости.

Естония

Многобройните кибератаки, предприети срещу съвременните информационни общества и насочени към подкопаване на функционирането на информационните системи на публичния и частния сектор, включиха злоупотребата с киберпространството в списъка на новите заплахи за сигурността. Осъзнаването, че подобни атаки представляват заплаха за международната сигурност, достига нови висоти за

[39] UN E-Government Survey 2016.

Естония през 2007 г. поради първата координирана кибератака срещу цяла страна, както и поради широкомащабни кибератаки срещу информационните системи и в много други страни. Повторното възникване и нарастващата честота на кибератаките показват началото на нова ера, в която сигурността на киберпространството придобива глобално измерение и защитата на критичните информационни системи трябва да бъде подобрена по отношение на националната сигурност, подобно на традиционните отбранителни интереси.[40]

Информационните технологии и свързаните в мрежата тясно преплетени услуги промениха из основи обществото в рамките на кратък период от време. По-голямата зависимост от електронните услуги доведе до по-голяма уязвимост в киберпространството. Естония разглежда тези въпроси в две национални стратегии за киберсигурност (2008 – 2013 г. и 2014 – 2017 г.). Първата национална стратегия за киберсигурност на Естония създаде вътрешни процедури и институции за осигуряване на ефективно разделение на задачите и сътрудничество между агенциите. Също така Естония подчертава необходимостта от сигурно киберпространство като цяло и се фокусира върху информационните системи. Препоръчаните мерки са от граждански характер и се концентрират върху регулирането, образованието и сътрудничеството. Последната стратегия поставя по-голям акцент върху защитата на критичната инфраструктура, борбата с киберпрестъпността и подобряването на компетентността за информационна сигурност. Също така развива законодателната среда с цел осигуряване на киберсигурност, международно сътрудничество и развитие на сектора за киберсигурност в икономиката. Настоящата стратегия е удължена до 2018 г., за да се допълнят изцяло целите за високо ниво на качество. Стартирана е подготовката за приемане на трета стратегия за киберсигурност. Тя ще помогне киберсигурността да бъде призната като по-широк приоритет за естонското общество. Тази нова стратегия ще се основава на предходната, като изложи ясна мисия и визия и добави стойност чрез междусекторни приоритети, като планира ресурсите, необходими за всички дейности.[41]

---

[40] Estonian National Cyber Security Strategy (2009).

[41] 18 May 2018, Republic of Estonia Ministry of foreign affairs, https://vm.ee/en/cyber-security.

България

На 31 октомври 2018 г. от 44-тото Народно събрание на Република България бе приет нов Закон за киберсигурност. Със закона се регламентират управлението и организацията на Националната система за киберсигурност, националният координатор по киберсигурност, секторни екипи за реакция при инциденти в киберсигурността, както и национален екип за реакция при инциденти в киберсигурността. С него се поставят основите на създаването на ефективна система за превенция и борба с кибератаките и за ограничаване на мащаба, честотата и въздействието на инцидентите в киберпространството. В закона са заложени мерки срещу инциденти, които причиняват големи икономически вреди и подкопават доверието на потребителите. Въвеждат се изисквания за сигурност, на които операторите и доставчиците на цифрови услуги трябва да отговарят. Предвижда се създаване на Национално единно звено за контакт, както и на национален екип за реакция при инциденти в киберсигурността.

В дадения закон са предоставени някои дефиниции от предметната област, като:

„***Киберсигурност*** е състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура, или които могат да нарушат работата им. ***Киберсигурността*** включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана. ***Мрежова и информационна сигурност*** е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях“.

В Закона за киберсигурност не са подчертани ролята и необходимостта от култура на киберсигурност на гражданите и потребителите на киберпространството, но за разлика от Закона този проблем се разглежда в Националната стратегия за киберсигурност КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2020. Националната стратегия за киберсигурност е приета от Министерския съвет на Репуб-

лика България на 13 юли 2016 г. Стратегията изразява колективния ангажимент и отговорност на всички заинтересовани страни и волята на ръководството на Република България да осигури модерна рамка и стабилна среда за развитие на националната система за киберсигурност и постигане на отворено, безопасно и сигурно киберпространство. Визията за постигане на „Киберустойчива България 2020“ очертава етапите на развитие и израстване от постигането на базова информационна сигурност и киберхигиена до зряло информационно общество, способно да устои на киберзаплахи и хибридни заплахи във всички сфери. Стратегията определя модела и механизмите за координация на стратегическо, политическо, оперативно и техническо ниво, както и ефективна платформа за споделяне на информация и колективен отговор. Набелязани са цели и мерки в девет основни направления, както и широко прилагане на различни форми на публично-частни партньорства.

Друга разлика – в Националната стратегия за киберсигурност КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2020 се говори за устойчивост, а не за защитеност, както е в Закона за киберсигурност. Според мен устойчивостта е по-реално и възможно за постигане състояние в сравнение със защитеността и пълната сигурност. Явление като пълна сигурност трудно се постига, а в киберпространството според мен и не съществува. По това, което е разписано в Закона за киберсигурност, става ясно, че за постигане на защитеност в киберпространството се разчита на информационните системи, които да се противопоставят на кибератаките. Не трябва обаче да се забравя кой ще управлява тези информационни системи, а именно човекът, който стои зад тях, и неговата култура за киберсигурност. В стратегията се обръща внимание на необходимостта на гражданите от достоверна и надеждна информация в интернет пространството, както и от доверие и защита на персоналните им данни, защита на човешките права и свободи в киберпространството. Освен гражданите като потребители, и държавата все повече разчита на интернет като канал за предоставяне на информация и услуги, а именно развиващото се е-управление за прозрачен и широк контакт с обществото. Чрез електронното управление държавата пренася необратимо дейността си в напълно дигитална среда.

Според Стратегията за постигане на киберустойчивост на национално ниво се изискват координирани действия за постигане

на сигурност и надеждност на всички компоненти и активи на киберпространството: информация, технологии, хора и съоръжения, на дизайна и реализацията на комуникационните канали, услугите и системите за управлението им, тяхната свързаност и оперативна съвместимост.

Стратегията набелязва цели и мерки за развитие в девет ключови области:

1. Установяване и развитие на националната система за киберсигурност и устойчивост;

2. Мрежовата и информационната сигурност – фундамент на киберустойчивостта;

3. Защита и устойчивост на дигитално зависимите критични инфраструктури;

4. Подобряване на взаимодействието и споделянето на информация между държава, бизнес и общество;

5. Развитие и подобряване на регулаторната рамка;

6. Засилване на противодействието на киберпрестъпността;

7. Киберотбрана и защита на националната сигурност;

8. Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на киберсигурността;

9. Международно взаимодействие – кибердипломация и оперативно взаимодействие.

В точка 8 „Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на киберсигурността“ са поставени цели за постигане на висока осведоменост на всички целеви групи и еднакво разбиране и оценка за заплахите във връзка с нарастващата всеобща дигитална зависимост и необходимостта от адекватни мерки на всички нива за постигане на информационна и киберсигурност, развитие на обща киберкултура. Към целите също спада включване на аспекти на киберсигурността, придобиване на адекватни компетентности във всички нива и форми на образование и обучение и създаване на специалисти, подготвени кадри и лидери за сигурно и устойчиво развитие на дигиталната икономика, общество и държавно управление в цифровата ера. Част от мерките, които са заложени в стратегията КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2020 за постигане на горните цели, са: мерки за повишаване на киберкултурата и

отговорното използване на дигитален обмен на информация, предоставяне и използване на електронни услуги по цялата верига на доставки (малък, среден и голям бизнес, граждани) и създаване на добавена стойност, обща и споделена отговорност за киберхигиена – ефективно използване на механизмите и платформите за споделяне на информация. За това се залага на внедряването на елементи и програми за киберсигурност във всички нива на обучение – начално, средно образование, педагогически програми за обучение на учители и преподаватели, професионално и университетско образование и продължаващо обучение.

В приложенията на Националната стратегия е представен SWOT анализ на състоянието и предизвикателствата пред България в киберпространството. Две от посочените слаби страни са: *Ниска степен на образованост и разбиране на важността на киберсигурността* и *Ниска технологична култура в част от структурите на централната и местната изпълнителна власт*. Като възможност е включено *Системно развитие на информационната култура в училищата.* По този начин чрез Националната стратегия за киберсигурност КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2020 се акцентира върху елемента необходимост от формиране и развитие на култура за киберсигурност за постигане на отворено, безопасно и сигурно киберпространство.

Гърция

Гърция няма приета стратегия за киберсигурност или специално законодателство за киберсигурността. Правната и институционалната рамка, която поддържа киберсигурността, също е ограничена. Националният екип за реакция при компютърни инциденти, NCERT-GR, е ограничен до държавни институции и операторите на критична инфраструктура. В Гърция няма значителни публично-частни партньорства и правителството не се стреми активно да създава или да засили сътрудничеството си с частния сектор.

Въпреки това Гърция разполага с официално призната Национална служба срещу електронни атаки (NAAEA), чиято мисия е да участва в превенцията срещу електронни атаки в комуникационните мрежи, съоръженията за съхранение на данни и информационните системи. Освен това органът отговаря за обработката на данни и за уведомяването на компетентните органи.

Друга институция, занимаваща се с осигуряването на киберсигурността в Гърция, е Гръцкият център за киберпрестъпления (GCC), който е част от нововъзникващите координирани европейски усилия, като има за цел:

1. Напредък в киберобучението и университетското образование в Гърция;

2. Подобряване на изследванията в целеви области на престъпленията в киберпространството, като ботнети и кибератаки;

3. Мобилизирне на гръцкия избирателен район в областта на киберпрестъпленията;

4. Сътрудничество с подобни центрове, така че да се постигнат максимални резултати.

5. GCC планира да разгърне инициатива за обучение и образование в областта на киберпрестъпленията с две стъпки – от една страна, ще бъде разработен набор от университетски курсове, които да подобрят разбирането за киберпрестъпността на новото поколение учени и студенти по право; от друга страна, набор от краткосрочни курсове за обучение, насочени към служителите в областта, за да подобрят разбирането си за киберсигурност.

Комбинирането на опита на националната индустрия, академичните среди и правоприлагащите органи на ССЗ има за цел да насърчи най-съвременното изследване на киберпрестъпленията. Същевременно, като се възползва от отличните резултати от научните изследвания на своя консорциум, ССП се стреми да се превърне в център за върхови постижения в областта на изследванията в областта на киберпрестъпността.

Един от методите, върху който пада фокусът, е насърчаване и стимулиране на обучение в сферата на киберсигурността.

Обучение се насърчава, когато:

1. обучаемите се занимават с решаването на реални проблеми;

2. наличните знания се използват като основа за нови знания;

3. на учещия се демонстрират нови знания;

4. новите знания се прилагат от учещия се;

5. новите знания са интегрирани в средата на учещия се.

Обобщена Европейска платформа

Европейската комисия прие набор от законодателни предложения, по-специално относно мрежовата и информационната си-

гурност. За периода 2014 – 2020 г. са заделени повече от 600 милиона евро инвестиции на ЕС за научни изследвания и иновации за проекти за киберсигурност и се насърчава сътрудничеството в рамките на ЕС и с партньорите на световната сцена.

Комисията засили своя подход, като постави киберсигурността в центъра на своите политически приоритети: доверието и сигурността са в основата на стратегията за цифров единен пазар, представена през май 2015 г., докато борбата срещу киберпрестъпността е един от трите стълба на Европейската програма за сигурност, приета през април 2015 г.

През юли 2016 г., изпълнявайки тези стратегии, Комисията представи допълнителни мерки за стимулиране на индустрията за киберсигурност и за справяне с киберзаплахите.

Приемането от Европейския парламент на Директивата за сигурността на мрежовите и информационните системи (Директивата за МИС) през юли 2016 г. е друга важна стъпка към по-сигурна онлайн среда.

Основни цели на Комисията в областта на киберсигурността са:

• Увеличаване на способностите и сътрудничеството в областта на киберсигурността. Целта е да се осигурят възможности за киберсигурност на същото ниво на развитие във всички държави членки на ЕС и да се гарантира, че обменът на информация и сътрудничеството са ефективни, включително на трансгранично равнище;

• Превръщане на ЕС в силен участник в киберсигурността. Европа трябва да бъде по-амбициозна, за да развива конкурентното си предимство в областта на киберсигурността и да гарантира, че европейските граждани, предприятията, публичните администрации имат достъп до най-новите технологии за цифрова сигурност, които са оперативно съвместими, конкурентни, надеждни и зачитат основните права, включително правото на личен живот. Това също трябва да помогне да се възползват от процъфтяващия глобален пазар на киберсигурност. За да се постигне това, Европа трябва да преодолее сегашната фрагментация на пазара на киберсигурност и да насърчи европейската индустрия за киберсигурност;

• Включване на киберсигурността в политиките на ЕС. Целта е въвеждането на киберсигурност в бъдещите политически инициативи на ЕС от самото начало, по-специално по отношение на новите технологии и нововъзникващите сектори, като свързани авто-

мобили, интелигентни мрежи и интернет на нещата (IoT).

Европейската комисия представя няколко инициативи и допринася за редица ключови мерки за по-добра онлайн защита на европейците.

Стратегии на ЕС

Стратегия на ЕС за киберсигурност (2013 г.)

Европейската комисия и Европейската служба за външна дейност стартираха Стратегията на ЕС за киберсигурност през 2013 г. Стратегията очертава принципите, които ще ръководят действията на ЕС в тази област, например значението на достъпа до интернет и защитата на основните права онлайн. Тя определя пет приоритета:

1. Увеличаване на киберустойчивостта;

2. Драстично намаляване на киберпрестъпността;

3. Разработване на политика и способности на ЕС в областта на киберотбраната, свързани с общата политика за сигурност и отбрана;

4. Разработване на промишлени и технологични ресурси за киберсигурност;

5. Създаване на последователна международна политика в областта на киберпространството за ЕС и насърчаване на основните ценности на ЕС

Европейска програма за сигурност (2015 г.)

По-ефективната борба с киберпрестъпността е един от трите приоритета в новата Европейска програма за сигурност за периода 2015 –2020 г., приета от Комисията през април 2015 г. Киберпрестъпността изисква координиран отговор на европейско равнище.

Ето защо Европейската програма за сигурност предлага следните действия:

- Поставяне на нов акцент върху прилагането на съществуващите политики в областта на киберсигурността, атаките срещу информационните системи и борбата срещу сексуалната експлоатация на деца;
- Преразглеждане и евентуално разширяване на законодателството относно борбата с измамите и фалшифицирането на непарични платежни средства, за да се вземат предвид по-новите фор-

ми на престъпност и фалшифицирането на финансови инструменти като предложенията през 2016 г.;

• Преразглеждане на пречките за разследване на престъпления в областта на киберпрестъпността, по-специално по въпросите на компетентната юрисдикция и правила за достъп до доказателства и информация;

• Засилване на действията за изграждане на капацитет в областта на киберпространството чрез инструменти за външна помощ.

Стратегия за единен цифров пазар (2015 г.)

Доверието и сигурността са от съществено значение за извличането на ползи от цифровата икономика. Ето защо стратегията за единен цифров пазар, представена през май 2015 г., включва публично-частно партньорство (ПЧП) относно киберсигурността.

Партньорството е подписано на 5 юли 2016 г. от Комисията и Европейската организация за киберсигурност (ECSO) – сдружение, водено от промишлеността, което включва голямо разнообразие от заинтересовани страни, като големи компании и стартиращи предприятия, изследователски центрове, университети, крайни потребители, оператори, клъстери и асоциации, както и публични органи.

Целта на това партньорство е да стимулира европейската конкурентоспособност и да помогне за преодоляване на фрагментирането на пазара на киберсигурност чрез иновации, изграждане на доверие между държавите членки и индустриалните участници, както и за подпомагане на сближаването на секторите на търсенето и предлагането за продукти и решения в областта на киберсигурността.

Това партньорство ще допринесе за структурирането и координирането на цифровите индустриални ресурси за сигурност в Европа. То включва широк кръг от участници – от иновативни малки и средни предприятия до производители на компоненти и оборудване, оператори на критични инфраструктури и изследователски институти. Инициативата ще използва усилията на ЕС, националните, регионалните и частните усилия и ресурси, включително фондовете за научни изследвания и иновации, за увеличаване на инвестициите в киберсигурността.

В крайна сметка партньорството помага за:

• събиране на промишлени и публични ресурси за постигане на иновации в съответствие със съвместно договорената пътна карта за стратегически изследвания и иновации;

• фокусиране върху целеви технически приоритети, определени съвместно с индустрията;

• максимизиране на въздействието на наличните средства;

• осигуряване на видимост на европейските постижения в областта на научните изследвания и иновациите в киберсигурността.

Партньорството се подкрепя от фондовете на ЕС, които идват от Рамковата програма за научни изследвания и иновации „Хоризонт 2020“ (H2020) с обща инвестиция до 450 милиона евро до 2020 г. Комисията възнамерява да започне първите H2020 покани за представяне на предложения по киберсигурност ПЧП в първото тримесечие на 2017 г.

Съобщение относно укрепването на системата за киберустойчивост в Европа и насърчаването на конкурентоспособна и иновативна индустрия за киберсигурност (2016 г.)

Въз основа на стратегията на ЕС в областта на киберсигурността и стратегията за цифров единен пазар Комисията прие на 5 юли 2016 г. Съобщение „Укрепване на системата за киберустойчивост в Европа и насърчаване на конкурентоспособна и иновативна индустрия за киберсигурност“.

Тя включва набор от мерки, насочени към:

• Засилване на сътрудничеството в цяла Европа: Комисията насърчава държавите членки да се възползват максимално от механизмите за сътрудничество съгласно Директивата за МИС и да подобрят начина, по който работят заедно, за да се подготвят за мащабен киберинцидент. Това включва повече работа по обучение и подготовка за киберсигурност;

• Подкрепа за нововъзникващия единен пазар на продукти и услуги за киберсигурност в ЕС: например Комисията ще проучи възможността за създаване на рамка за сертифициране на съответните продукти и услуги на ИКТ, допълнена от доброволна и лека схема за етикетиране за сигурността на ИКТ продукти; Комисията предлага също възможни мерки за увеличаване на инвестициите в киберсигурността в Европа и за подкрепа на МСП, които са активни на пазара;

• Създаване на договорно публично-частно партньорство (ПЧП) с промишлеността за подхранване на индустриалния капацитет и иновациите в областта на киберсигурността в ЕС.

Законодателство на Европейския съюз

Директива за мрежова и информационна сигурност

През 2013 г. Комисията предложи Директива относно сигурността на мрежовите и информационните системи (Директива за МИС), чиято цел е да осигури високо общо ниво на киберсигурност в ЕС. На 7 декември 2015 г. преговарящите от Европейския парламент, Съвета и Комисията постигнаха съгласие по текста (http://europa.eu/rapid/press-release_IP-15-6270_en.htm).

След политическото споразумение, постигнато на 7 декември 2015 г., текстът на Директивата за МИС беше приет от Европейския парламент на 6 юли 2016 г. и влезе в сила през август 2016 г. Държавите членки имат 21 месеца, за да внедрят Директивата в своите национални законодателства и още 6 месеца, за да се идентифицират операторите на основни услуги.

Директивата се основава на три основни стълба:

• Осигуряване на готовност на държавите членки, като се изисква те да бъдат подходящо оборудвани, например чрез екип за реагиране на инциденти в областта на компютърната сигурност (CSIRT) и компетентен национален орган за МИС;

• Осигуряване на сътрудничество между всички държави членки чрез създаване на „група за сътрудничество“ с цел подпомагане и улесняване на стратегическото сътрудничество и обмена на информация между държавите членки, както и „мрежа на ЦДКСКС“ с цел насърчаване на бързото и ефективно функциониране на сътрудничество по конкретни инциденти в киберсигурността и споделяне на информация за рисковете;

• Осигуряване на култура на сигурност в секторите, които са жизненоважни за нашата икономика и общество и освен това зависят в голяма степен от информационните и комуникационните технологии (ИКТ). Предприятията с важна роля за обществото и икономиката, които са идентифицирани от държавите членки като оператори на основни услуги съгласно Директивата за МИС, ще трябва да предприемат подходящи мерки за сигурност и да съоб-

щават за сериозни инциденти на съответния национален орган. Тези сектори включват енергетика, транспорт, вода, банкиране, инфраструктури на финансовите пазари, здравеопазване и цифрова инфраструктура;

• Също така ключовите доставчици на цифрови услуги (търсачки, услуги за изчислителни облаци и онлайн пазари) ще трябва да отговарят на изискванията за сигурност и уведомяване съгласно новата директива. Подобни изисквания вече се прилагат за телекомуникационните оператори и доставчиците на интернет услуги чрез телекомуникациите регулаторната рамка на ЕС.

Общ преглед за стратегиите

Както на вътрешноевропейско, така и на международно равнище явно липсва хармонизирана дефиниция за киберсигурност. Разбирането на киберсигурността и други ключови термини варира значително в различните страни. Това влияе върху различните подходи към стратегията за киберсигурност сред страните в целия свят. Липсата на общи разбирания и подходи може да възпрепятства международното сътрудничество, чиято необходимост се признава от всички страни.

В заключение можем да направим извода, че основните точки, обхванати от типичните национални стратегии за киберсигурност, обикновено са в рамките на:

• Определяне на управленска рамка за киберсигурност;

• Определяне на подходящ механизъм (често публично-частно партньорство), който позволява на всички съответни публични и частни заинтересовани страни да обсъждат и съгласуват различни въпроси на политиката и регулаторната киберсигурност;

• Очертаване и определяне на необходимите политики и регулаторни мерки и ясно определени роли, отговорности и права на частния и публичния сектор (например нова правна рамка за борба с киберпрестъпността, задължително докладване на инциденти, минимални мерки за сигурност и насоки, нови правила за възлагане на обществени поръчки). Например стратегията на Словакия идентифицира необходимостта от определяне на правна рамка за защита на киберпространството;

• Определяне на целите и средствата за развитие на националните способности и необходимата правна рамка за участие в

международните усилия за намаляване на последиците от киберпрестъпността. В няколко стратегии се обръща специално внимание на киберпрестъпността. Например в Холандия, която има за цел да засили разследването и преследването на киберпрестъпления. Франция също подчертава тази точка и желае да насърчи укрепването на действащото законодателство и международното съдебно сътрудничество;

• Идентифициране на критични информационни инфраструктури, включително ключови активи, услуги и взаимозависимости;

• Разработване или подобряване на плановете за подготовка, реагиране и възстановяване, както и на националните планове за действие при извънредни ситуации, киберупражнения и осведоменост за ситуацията. Литовската стратегия гласи: „За да се гарантира сигурността в киберпространството, е необходимо да се създаде непрекъсната и правилно управлявана система, обхващаща всички фази на управлението на инциденти, като ранно предупреждение, предотвратяване, разкриване, елиминиране и разследване“. Това включва и определяне на интегрирани организационни структури, които разработват, прилагат и тестват плановете и мерките за готовност, реакция и възстановяване. Това може да означава и интеграция на съществуващи структури (например национални/правителствени CERT);

• Определяне на систематичен и интегриран подход към националното управление на риска (например споделяне на надеждна информация и национални регистри на рисковете);

• Дефиниране и определяне на целите на кампании за повишаване на осведомеността, които променят поведението и моделите на работа на потребителите;

• Определяне на нуждите от нови учебни програми с акцент върху киберсигурността за ИТ специалисти и специалисти по сигурността; както и от програми за обучение, които позволяват подобряване на уменията на потребителите. Например стратегията на Обединеното кралство има за цел да подобри обучението и образованието на специалистите по информационна сигурност, за да създаде силна професия за киберсигурност;

• Международно сътрудничество с ЕС и държави извън ЕС (например приемане на международни конвенции).

Ако си поставим за цел да екстраполираме развитието на науката и практиката в това направление, то със сигурност бихме могли да твърдим, че следващите крачки тук ще са свързани с научноизследователски и развойни програми, които се фокусират върху нововъзникващи проблеми, свързани със сигурността и устойчивостта, както и с бъдещи интелигентни системи, устройства и услуги.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. **Агамирзян**, И. Электронное правительство в контексте глобализации, 2002. Достъпно на: http://www.computer.ru/offline/2002/448/18414,
2. Академия, 2003.
3. **Анилина**, М. И. Философия современной библиотеки. – В: *Библиотековедение*, 1996, № 4/5, с. 91 – 100.
4. **Арменчечва**, Илина. Стратегиите за киберсигурност в ЕС като елемент от политиката за национална и международна сигурност. – Във: *Военен журнал*, бр. 3, 2014.
5. **Базин**, Швета. Основи на мрежовата сигурност. s.l.: ДуоДизайн, 2004.
6. **Бауман**, З. Глобализацията: Последиците за човека. София: ЛИК, 1999.
7. **Босакова**, Кристина. Човешкият фактор в системите за сигурност. – В: **Интернет** либерализацията – предизвикателства и добри практики пред интелектуалната собственост. Сборник с доклади от IV национален семинар с международно участие, 26 – 27 април 2016 г. София: За буквите – О писменехь, с. 387 – 390.
8. **Бърнев**, П. Информация и управление. София: Народна просвета, 1978.
9. **Владков**, Владимир. Киберсигурността – сред най-важните теми по време на българското председателство на ЕС. Computerworld [Online]. септември 28, 2017 [Cited: септември 12, 2018]. http://computerworld.bg/51625_kibersigurnostta__sred_najvazhnite_temi_po_vreme_na_balgarskoto_predsedatelstvo_na_es.
10. **Вълчев**, Г. Приоритизацията на инициативите за е-Правителство следва утвърдена методология. – В: *CIO*, 2005, № 1, с. 18.
11. **Генов**, Н. Социологията и социалното развитие. – В: **Перспективи** пред социологията в България. София: УИ „Св. Климент Охридски“, 2001, с. 1 – 45.

12. **Геров**, А. Ролята на неправителствените организации в информационното общество. – В: *Информационно общество*, 3 – 5 ноември 1998 г. София, 1998, с. 79 – 81.
13. **Гончаренко**, Н. Справочное бюро для администрации. – В: *Библиотека*, 2001, № 8, с. 26 – 27.
14. **Горман**, М. Нашите непреходни ценности. Библиотеките през XXI век. София: УИ „Св. Климент Охридски“, 2006.
15. **Гудман**, Марк. Киберпрестъпления. Всичко е свързано, всеки е уязвим и как да се защитим. s.l.: Милениум, 2016.
16. **Далмън**, К. Концепцията на Световната банка за икономиката на знанието, 2003. Достъпно на: http://www.bgrazvitie.net/bg/ke/browser.php?state=content&cat_id=38&type=link
17. **Делибеев**, И. Теория и методика на емпиричното социологическо изследване. София, 1987.
18. **Денчев**, С. Информационна среда за трансфер на технологии. Кн. 1. София: Захарий Стоянов, 2003.
19. **Денчев**, С., Д. **Христозов**. Информиране и информационно брокерство. София: АИ „Проф. Марин Дринов“, 2012.
20. **Денчев**, С., Д. **Христозов**. Несигурност, сложност и информация. Анализ и развитие на несигурна информационна среда. Кн. 2. София: Захарий Стоянов, 2004.
21. **Денчев**, С., М. **Павлова**. Университетският имидж – фактор за генериране на доверие в образователната институция. – В: *Образование и технологии.* Бр. 9/2018, Издание 1, с. 61 – 63.
22. **Денчев**, С., И. **Петева**. Библиотеки и публичен достъп до информация. София: За буквите – О писменехь, 2006.
23. **Денчева**, К. Интелектуални комуникации и съвременни технологии. София: АИ „Проф. Марин Дринов“, 2003.
24. **Димчев**, А. Общодостъпните библиотеки и шансовете им за бъдещето. – В*: Библиотека*, 2003, № 4 – 5, с. 5 – 11.
25. **Димчев**, А. Предизвикателствата пред библиотеките в информационното общество: На примера на публичните библиотеки. – В: **Живот** сред хората. Юбилеен сборник в чест на проф. д-р Е. Савова. Съставител Нели Костова. София, 2004, с. 160 – 166.
26. **Добрев**, Б., Е. **Гецова**. Пътеводител за електронно правителство. София: International university, 2005, с. 317.

27. **Дуранкев**, Георги. Най-големите кибератаки през 2018 (досега). Freedomonline. [Online] август 02, 2018. [Cited: септември 12, 2018], https://freedomonline.bg/nay-golemite-kiber-ataki-prez-2018-dosega/.
28. **е-Община 2005.** София, Фондация „Приложни изследвания и комуникации“. Достъпно на: http://www.arc.online.bg/fileSrc.php?id=1634
29. **Зелена** книга на ЕС: Живот и труд в информационното общество: Хората на преден план = Green paper: Living and working in the Information society: People First. Достъпно на: http://www.ispo.cec.be/infosoc/legreg/docs/peoplıst.html
30. **Икономика** на знанието. София: Фондация „Приложни изследвания и комуникации“, 2004. Достъпно на: http://www.arc.online.bg/fileSrc.php?id=508
31. **Информационно-библиотечная** сфера: Международые акты и рекоммендации: Сб. справочно-нормативных и рекомендательных материалов. Составители: Е. И. Кузмин, В. Р. Фирсов. Москва: Либрея, 2001.
32. **Йотов**, Ст. Етика и мултикултурализъм. София: Агата-А, 2003.
33. **Камерон**, К., Р. **Куинн**. Диагностика и изменение организационной культуры, 2001.
34. **Кантарджиев**, А. Информационна философия. Варна: ВСУ „Черноризец Храбър“, 2004.
35. **Каплан**, Р. Д. **Нортън**. Стратегически карти. Да приведем нематериалните активи в осезаеми резултати. София: Класика и Стил, 2006.
36. **Кастелс**, М. Възходът на мрежовото общество. София: ЛИК, 2004.
37. **Кастелс**, М. Силата на идентичността. София: ЛИК, 2006.
38. **Кискинов**, В. Електронно правителство. София: Сиби, 2003.
39. **Кискинов**, В. Систематика на правната информатика. София: Сиби, 2003.
40. **Концепция** и политика за информационна сигурност: Защита на класифицираната информация в компютърни системи за управление при бедствия, аварии и катастрофи. Част 1. Стоян Денчев, Цветан Семерджиев, Иван Попов, Нели Костова. София: За буквите – О писменехь, 2006.

41. **Кросби**, Б. и др. Учения за лобиране за реформи в политиката. – В: *Демократичен преглед*, 1998, № 36, с. 240 – 244.
42. **Лазов**, Иван. Киберсигурността оттук нататък ще става още по-важна за всеки европейски гражданин. БНР, Радио Благоевград. [Online] май 14, 2018. [Cited: септември 12, 2018], http://bnr.bg/blagoevgrad/post/100970582.
43. **Леонова**, В. Пространство библиотеки. Москва: Наука, 2003.
44. **Лепскин**, В. Становление стратегических субектов в глобалном информационном обществе: Постановка проблеммы. – В: *Информационное общество*, Москва, № 4, с. 50 – 58.
45. **Лукас**, А. Предоставяне на административни услуги посредством системата за обслужване на едно гише – международна перспектива. – В: *Публична администрация*, кн. 1, 2002.
46. **Манасиева**, Астра. Киберпсихология. Поведенчески аспекти. s.l.: Изток-Запад, 2016.
47. **Манойло**, А. В. Государственная информационная политика в особых условиях. Москва, МИФИ, 2003.
48. **Михнова**, И. Библиотека как информационный центр для населения: Проблемы и их решения. Практ. пособие. Москва: Либрея, 2000, 128 с.
49. **Национална** програма за развитие на Информационното общество 1999 – 2006. Достъпно на: http://www.evroportal.bg/article_view.php?id=675528
50. **Национална** стратегия за развитие на информационното общество, декември 1998 г. Достъпно на: http://www.bild.net/infosoc/docs/strategy.htm
51. **Николова**, Н. Индивидуализация и социална интеграция в изграждането на информационно общество. – В: **Перспективи** пред социологията в България. София: УИ „Св. Климент Охридски", 2001, с. 395 – 414.
52. **Окинавска** харта за глобално информационно общество = Okinawa Charter on Global Information Society. Достъпно на: http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm
53. **Панайотова**, Е. Достъп до обществена информация. София: Сиби, 2003.
54. **Парсънс**, Т. Еволюцията на обществата. София: Критика и хуманизъм, 1998.

55. **Персикова**, Т. Межкультурная коммуникация и корпоративная культура. Москва: Логос, 2002.
56. **Петев**, Т. Теории за масовата комуникация. София: СУ „Св. Климент Охридски", 2004.
57. **Петева**, И. Дигитальная изоляция – библиотека – електронное правительство. – В: **Роль** книгоиздания в развитии международных научных и культурных контактов. Москва: Наука, 2005, с. 134 – 136.
58. **Петева**, И. Изграждането на е-Центрове на базата на общодостъпните библиотеки – средство за осигуряване на равнопоставен достъп до информация и услуги на гражданите и бизнеса. – В: **Трудове** на СВУБИТ, 3. София: За буквите – О писменехь, 2004.
59. **Петева**, И. Факторы, определяющие место библиотек при реализации э-Правительства в Болгарии. – В: **Книжная** культура. Опыт прошлого и проблемы современности. Москва: Наука, 2005.
60. **План** за действие: Европа – път към Информационното общество. Достъпно на: http://europa.eu.int/information_society/eeurope/plus/action_plan/index_en.htm
61. **Попов**, И. Социология, сигурност, информация. София: Полицейска академия, 2003.
62. **Разроев**, Э. Инфокоммуникационный бизнес: Управление, технологии, маркетинг. Санкт-Петербург: Професия, 2003.
63. **Рифкин**, Дж. Епоха на достъпа. София: Атика, 2001.
64. **Саръев**, И., Ц. **Семерджиев.** Архитектурен подход – методология на промените. – Във: *Военен журнал*, 2004, № 6, с. 97 – 108.
65. **Семерджиев**, Цв. Сигурност и защита на информацията. s.l.: Класика и Стил, 2007.
66. **Семерджиев**, Цв. Стратегическо ръководство и лидерство: Организации. София: Софттрейд, 2007.
67. **Семерджиев**, Цв. Стратегия: Среда, ресурси, способности, планиране. София: Класика и Стил, 2007.
68. **Соколов**, А. Социальные функции библиотечной и библиографической деятельности. – В: *Науч. и техн. библиотеки*, 1984, № 6, с. 19 – 27.

69. **Соуни**, М., Р. **Уолкът**. Седемте мита за иновацията. Достъпно на: http://mediatimesreview.com/february05/Inovation.php
70. **Столяров**, Ю. Сущностно-функциональный анализ библиотеки как системы – теоретико-методологическая основа повышения эффективности и качества библиотечного обслуживания. Автореф. дис. докт. педаг. наук. Москва, 1982, с. 29.
71. **Столяров**, Ю. Что такое библиотека? (О ее сущности и исходных функциях). – В: *Библиотековедение,* 1999, № 7, с. 20 – 33.
72. **Суслова**, И., В. **Кармовский**. Менеджмент в современной библиотеке. Науч.-метод. пособие. Москва: Амберея, 2004.
73. **Тофлър**, А. Третата вълна. София: П. Яворов, 1991.
74. **Тофлър**, А., Х. **Тофлър**. Новата цивилизация. София: Обсидиан, 1995.
75. **Трифонов**, Р. Административните е-услуги преминават към „двупосочно взаимодействие". – В: *CIO*, 2005, № 1.
76. **Трифонов**, Р. Електронно правителство – състояние и перспективи. Достъпно на: http://www.bait.bg/docs/Presentation%20_Trifonov.ppt
77. **Уэбстер**, Ф. Теории информационного общества. Москва: Аспект Прес, 2004.
78. **Фирсов**, В. Р. Сущностные функции библиотечной деятельности. Культуролог. подход. – В: *Науч. и техн. библиотеки.* Москва, 1985, № 5, с. 15 – 20.
79. **Хабермас**, Ю. Морал, право и демокрация. София, 1999.
80. **Холмс**, Д. Стратегии за електронно правителство. София: Класика и Стил, 2002.
81. **Христозов**, Д., С. **Денчев**. Информационно брокерство. София: WINI-1873, 2004, с. 201.
82. **Цветкова**, М. Информационната култура като фактор на писмената цивилизация. 2001. Достъпно на: http://www.lib.bg/dokladi2001/milena2.htm
83. **Цеков**, Иво. Анализ: Киберпространството като ново поле на противопоставяне. 2018.
84. **Целков**, В., Н. **Стоянов**, О. **Исмаилов**. Управление на риска, тестване и оценка на мрежовата и информационна сигурност. s.l. София: За буквите – О писменехь, 2016.

85. **Чачко**, А. Развивающаяся библиотека в информационном обществе: Научно-методическое пособие. Москва: Либрея, 2004.
86. **Шевчук**, О. Виртуальная основа реального государства.
87. **Шрайберг**, Я. Роль библиотек в преобразовании гражданского общества в информационное. – В: *Науч. и техн. библиотеки*, 2000, № 4, с. 83 – 92.
88. **Юнг**, К. Човекът и неговите символи. София, 2002.
89. **Янкова**, И. Модерната библиотека: Мястото на съвременната библиотека в съвременното образование. София: УИ „Св. Климент Охридски", 2004.
90. **Яновский**, Р. Г. Глобальная информатизация и гуманитарные проблемы. – В: **Глобальная** информатизация и безопасность России: Материалы «круглого стола» «Глобальна информатизация и социально-гуманитарные проблемы человека, культуры, общества». Под ред. профессора В. И. Добренькова. Москва, 2001.

91. **A National** Strategy for an Effective Cybersecurity Approach and. Ghernaouti, Solange, 2010.
92. **Abbott**, H., E. **Bernadine**. Government Publications Library of Last Resort. – In: *Unabashed Librarian*, 2004, Issue 131, pp. 5 – 16.
93. **Akerlof**, George A. The Market for 'Lemon's: Quality Uncertainty and the Market Mechanism. – In: *Quarterly Journal of Economics* 84(3), 1970, pp. 488 – 500.
94. **Akeroyd**, R. White House Conference on Library and Information Services: Expand Literacy, Increase Productivity, Strengthen Democracy. – In: *Library Admistration and Management*, 1991, 5(2), p. 1 – 72.
95. **Alavi**, M., D. **Leidner**. Knowledge Management and Knowledge Management Systems: Conceptual Foundation and an Agenda for Research. MIS Quarterly, March 2001.
96. **Ansoff**, Igor. Corporate Strategy. McGraw Hill, New York, 1965.
97. **Bandura**, A. Social Learning Theory. Englewood Cliffs, NJ: Prentice-Hall, 1997.
98. **Barnard**, Chester. The function of the executive. Harvard University Press, Cambridge Mass, 1938, 235 p.

99. **Barney**, J. Firm Resources and Sustainable Competitive Advantage. – In: *Journal of Management*, vol 17, no 1, 1991.
100. **Bartlett**, C., S. **Ghoshal**. Changing the Role of Top Management. Harvard Business Review, May/Jun, 1995.
101. **Barton**, D. L. Wellsprings of Knowledge. Harvard Business School Press, Boston, 1995.
102. **Benton** Foundation. Strategic Communications in the digital age: A best practices toolkit for achieving your organization's mission. Available from www.benton.org/publibrary/toolkits/stratcommtool.html.
103. **Berkowitz**, Stephen D. An Introduction to Structural Analysis: The Network Approach to Social Research. Toronto: Butterworth, 1982.
104. **Berry**, L. On Great Service. Free Press, New York, 1995.
105. **Berryman**, J. E-government: issues and implications for public libraries. – In: *Australian Library Journal*, Vol. 53, 2004, Issue 4, pp. 349 – 359.
106. **Bivins**, Thomas H. *Handbook for Public Relations Writing*. Chicago: NTC Business Books, 1999.
107. **Blake**, M. The information society. – In: *Electronic Library*, Vol. 21, 2003, Issue 4, pp. 389 – 392.
108. **Blaxill**, Mark, Ralph **Eckardt**. The Invisible Edge: Taking your Strategy to the Next Level Using Intellectual Property (Portfolio, March 2009).
109. **Bolt**, N. Libraries, public policy, and economic development. – In: *Library Administration and Management*, 1991, 5(2), pp. 81 – 85.
110. **Bourdon**, C. Librarian's Library. – In: *American Libraries*, Vol. 34, Oct 2003, Issue 9, p. 76 – 77.
111. **Brandes**, Ulrik, Thomas **Erlebach** (Eds.). Network Analysis: Methodological Foundations Berlin, Heidelberg: Springer-Verlag, 2005.
112. **Breiger**, Ronald L. The Analysis of Social Networks in Handbook of Data Analysis. Edited by Melissa Hardy and Alan Bryman. London: Sage Publications, 2004, pp. 505 – 526.
113. **Bunyan**, T. Secrecy and openness in the European Union – the ongoing struggle for freedom of information. [Online], http://www.statewatch.org/secret/freeinfo/index.html

114. **Burson-Marstellers** and **B.K.S.H.** The definitive guide to lobbying the European institutions. Brussels, 2005. Available in: http://www.bmbrussels.be/files/file-70.pdf
115. **Buzzell**, R., B. **Gale**. The PIMS Principles: Linking Strategy to Performance. Free Press, New York, 1987.
116. **Carnaby**, P. Reading the changes: a view on the revitalised public sector in New Zealand. – In: *New Zealand Libraries*, Vol. 49, 2003, Issue 9, pp. 99 – 300.
117. **Carnegie** Mellon University. Information Security Essentials. Computing Services Information Security Office. [Online], https://www.cmu.edu/iso/aware/presentation/tepperphd.pdf
118. **Carpenter**, K. Government Publications and the Development of Libraries. – In: *Alexandria*, Vol. 15, 2003, Issue 1, pp. 49 – 62.
119. **Carrington**, Peter J. Models and Methods in Social Network Analysis. John Scott and Stanley Wasserman (Eds.). New York: Cambridge University Press, 2005.
120. **Castells**, Manuel. The Rise of the Networked Society: The information age. Blackwell Publishers, Cambridge Mass, 1996.
121. **Chaffee**, E. Three models of strategy. Academy of Management Review, vol 10, no. 1, 1985.
122. **Chandler**, Alfred. Strategy and Structure: Chapters in the history of industrial enterprise. Doubleday: New York, 1962.
123. **Chang-HyunJin.** Self-concepts in cyber censorship awareness and privacy risk perceptions: What do cyber asylum-seekers have? – In: **Computers** in Human Behavior, Vol. 80, 2018.
124. **Chang-Tseh**, Hseih, Fujun **Lai**, Weihua **Shi**. Information orientation and its impact on information asymmetry and e-business adoption: Evidence from China's international trading industry, Industrial Management & Data Systems, 106 (6), 2006, pp. 825 – 840.
125. **Christozov**, D., P. **Mateev**. Assessment of Information Assymetry. – In: **Pliska** Studia Mathematica Bulgarica, Vol. 17, 2005, pp. 27 – 38.
126. **Christozov,** D., P. **Mateev**. Warranty as a Factor for e-Commerce Success, Informing Science and IT Education Conference, Pori, Finland, June 2003.
127. **Christozov**, D., S. **Chukova**, P. **Mateev**. A Measure of Risk Caused by Information Asymmetry in e-Commerce. – In: *Journal of Issues in Informing Science and Information Technology*, Volume 3, 2006, pp. 147.

128. **Christozov**, D., S. **Chukova**, P. **Mateev**. Assessment of Quality of Warranty Policy. – In: *Interdisciplinary Journal of Information, Knowledge, and Management*, Volume 5, 2010, pp. 62 – 72.
129. **Christozov**, D., S. **Chukova**, P. **Mateev**. Assessment of Risk of Misinforming: Dynamic Measures. – In: *Interdisciplinary Journal of Information, Knowledge, and Management*, Volume 6, 2011, pp. 163 – 176.
130. **Christozov**, D., S. **Chukova**, P. **Mateev**. On the Relationship between Warranty and the Risk of Information Asymmetry. – In: *Journal of Issues in Informing Science and Information Technology*, Volume 4, 2007, pp. 235 – 249.
131. **Christozov**, D., S. **Chukova**, P. **Mateev**. On two types of warranties: warranty of malfunctioning and warranty of misinforming. – In: *Asia-Pacific Journal on Operation research*, Vol. 26, No. 3, 2009, pp. 399 – 420.
132. **Christozov**, D., S. **Chukova**, P. **Mateev**. Warranty and the Risk of Misinforming: Evaluation of the Degree of Acceptance. – In: *Journal of Issues in Informing Science and Information Technology*, Volume 5, 2008, pp. 667 – 677.
133. **Cohen**, E. Reconceptualizing Information Systems as a Field of the Discipline Informing Science: From Ugly Duckling to Swan. – In: **Gill**, G., E. **Cohen** (editors). Foundation of Informing Science: 1999 – 2008, Informing Science Press, 2009, pp. 7 – 20.
134. **Cook**, Meghan E. What Citizens Want From e-government. Center for Technology in Government: University at Albany. Available in: http://www.ctg.albany.edu/resources/htmlrpt/egovernment/what_citizens_want.html
135. **Corner**, P., A. **Kinicki**, B. **Keats**. Integrating organizational and individual information processing perspectives on choice. – In: *Organizational Science*, vol. 3, 1994.
136. **Crainer**, Stuart, Des **Dearlove**. Whatever Happened to Yesterday's Bright Ideas? – In: *Across the Board*, Vol. 43, No. 3, May/June 2006, pp. 34 – 40.
137. **Crosby**, P. Quality is Free. McGraw Hill, New York, 1979.
138. **Daft**, R. E., K. E. **Weick**. Toward A Model of Organizations as Interpretation Systems. – In: *Academy of Management Review*, 9, 1984.
139. **Davenport**, T. H., D. W. **De Long,** M. C. **Beers**. Successful Knowledge Management. – In: *Sloan Management Review*, 39, 2, 1998.

140. **Davis**, R., I. **Trohopoulos**. Public Libraries, Public Information, Digital Literacy and Citizen. – In: **Libraries** in the Age of the Internet. Papers from the International Conference held in Sofia, Bulgaria, 8 – 10 November 2000, Sofia, 2001, pp. 51 – 71.
141. **Deal**, T. E., A. A. **Kennedy**. Corporate Cultures: The Rites and Rituals of Corporate Life. Reading, Mass, 1982.
142. **Denchev**, S. Information technology and challenges to the nation. – In: **Annual** of "Informatics" Section Union of Scientists in Bulgaria, Volume 1, 2008, pp. 3 – 12 [Language: BG].
143. **Denchev**, S. Alternative university educational models in the knowledge society. – In: **Contemporary** strategies and innovations in the knowledge management. Sofia, Za Bukvite – O Pismeneh, 2014, pp. 55 – 69 [Language: BG].
144. **Denchev**, S., I. **Pavlova**. Analysis and management of university information environment. Sofia, Za Bukvite – O Pismeneh, 2010, 213 p. [Language: BG].
145. **Denchev**, S., I. **Peteva**. The Libraries – Local Authorities Partners in the Realization of e-Government of Bulgaria. – In: **The Economic** Role of Libraries in Modern Society, Belgrade, 2005.
146. **Denchev**, S., I. **Peteva**, D. **Stoyanova**. An Innovative Method for Knowledge Diffusion – Powerful Instrument for Enhancing Students' Motivation. – In: **Proceedings** of the New Perspectives in Science Education (Florence, 17 – 18 March, 2016), pp. 101 – 104.
147. **Denchev**, S., T. **Trencheva**. The Summer Knowledge Academy as a Part of the University Research and Educational Environment. – In: **Proceedings** of the International Conference: The New Perspectives in Science Education (Florence, Italy, March 20 – 21, 2015). Simonelli Ed., Vol. 4, pp. 262 – 265.
148. **Denison**, D. R., A. K. **Mishra**. Organizational Culture and Effectiveness. – In: *Organization Science*, 6, 2, 1995.
149. **Drucker,** P. The Age of Discontinuity. Heinemann, London, 1969 (also Harper and Row, New York, 1968).
150. **Drucker**, P. The coming of the new organization. – In: *Harvard Business Review*, 1988, January-February, pp. 45 – 53.
151. **Drucker**, P. The Practice of Management. Harper and Row. New York, 1954.
152. **E-Europe 2005** Action Plan: eEurope 2005: a society for all, http://europa.eu.int/information_society/eeurope/2002/news_lib

rary/documents/eeurope2005/eeurope2005_en.pdf
153. **eEurope 2005**, http://europa.eu.int/comm/information_society/europe/index_en.htm
154. **E-Government** – A Vision for New Zealanders. E-government Unit of the State Services Commission (2000), http://www.govt.nz/evision/index.php3
155. **E-Government** Handbook for Developing Countries, http://www.cdt.org/egov/handbook
156. **e-Government** Interoperability Framework. www.govtalk.gov.uk/documents/ e-GIF4Pt1_draft_2002-03 07_ formatted pdf
157. **E-government** Leadership: Engaging the Customer Accenture, 2003. www.accenture.com/xdoc/en/industries/government/gove_capa_egov_leaders
158. **E-Government ovt** Act Passed, But ALA is Wary. – In: *Library Journal*, December 24, 2002.
159. **e-Government** Role of UK Online Centres April 2005. Available at: www.egovmonitor.com/node/346
160. **E-Government** Usability for Older Adults. – In: *Communications of the ACM*, Vol. 48, 2005, Issue 2, pp. 102 – 104.
161. **Elcock**, Howard. Strategic Management. – In: **Farnham**, D. and S. **Horton** (eds.). Managing the New Public Services. 2nd Edition. New York: Macmillan, 1996, p. 56.
162. **Elmasri**, R. and S. **Navathe**. Database Systems: Models, Languages, Design and Application Programming. Sixth edition, Pearson, 2011.
163. **Engaging** Citizens Online for Better Policy-Making. [Online], http://www.oecd.org/dataoecd/62/23/2501856.pdf
164. **Eve**, J., P. **Brophy**. The Value and Impact of IT Access in Public Libraries: Final Report. – In: **Center** for Research in Library and Information Management, http://www.cerlim.ac.uk
165. **Eve**, J., P. **Brophy**. VITAL issues: the perception, and use, of ICT servicing UK public libraries, LIBRES. – In: *Library and Information Science Research (Electronic Journal)*, 2000, Vol. 10, Issue 2, http://aztec.lib.utk.edu/libres/libre10n2/vital.htm
166. **Evens**, P., T. **Wurster**. Strategy and the New Economics of

Information. – In: *Harvard Business Review*, Sept/Oct 1997.
167. **Expanding** the Information Society in Ireland: Report to the Information Society Commission. Dublin, 2003, www.isc.ie
168. **Falling** Through the Net: Defining the Digital Divide. (1999). Retrieved June 16, 2004. [Online], http://www.ntia.doc.gov/ntiahome/fttn99/contents.html
169. **Feignbaum**, A. Total Quality Control. 3rd edition. McGraw Hill, Maidenhead, 1990.
170. **Fell**, Gregory, Mike **Barlow**. Who Are the Bad Guys and What Do They Want? 1005 Gravenstein Highway North, Sebastopol, CA: O'Reilly Media, Inc., March 2016.
171. **Framework** for the Future: Libraries, Learning and Information in the Next Decade United Kingdom, Department for Culture, Media and Sport, 2003. [Online], http://www.culture.gov.uk/heritage/pl_framework.html
172. **Frank**, R., P. **Cook**. The Winner Take All Society. Free Press. New York, 1995.
173. **Freeman**, C. Linton. The Development of Social Network Analysis: A Study in the Sociology of Science. Vancouver: Empirical Press, 2004.
174. **Freeman**, Linton. The Development of Social Network Analysis. Vancouver: Empirical Pres, 2006; **Wellman**, Barry and S. D. **Berkowitz**, eds., 1988. Social Structures: A Network Approach. Cambridge: Cambridge University Press, 2006.
175. **Froud**, R., Ch. **Mackenzie**. E-Government & public libraries: Promoting local and national agendas. Gütersloh, Bertelsmann Foundation, 2002. [Online], http://www.publiclibraries.net/html/x_media/pdf/e_government_engl.pdf
176. **Furger**, Roberta. Internet filters: the smut stops here. Or does it? Screening five top Web filters. – In: *Personal Computer World* (U.S.A.), October 1997, pp. 78 – 80.
177. **Gackowski**, Z. Informing Systems for Operations: A Teleological View. – In: **Gill**, G., E. **Cohen** (editors). Foundation of Informing Science: 1999 – 2008. – In: *Informing Science Press*, 2009, pp. 57 – 112.
178. **Gackowski**, Z. Quality of Informing: Credibility – A provisional model of functional dependences – In: *Informing Science: The International Journal of Emerging Transdiscipline*, Vol. 9, 2006, pp. 225 – 241.

179. **Gladwell**, Malcolm. The Tipping Point. New York: Little Brown, 2000.
180. **Golderman**, G ., Br. **Connolly**. Government information online: tools for democracy. – In: *Library Journal*, 2002, pp. 50 – 55.
181. **Habermas**, J. Between Facts and Norms. Contribution to a Discourse Theory of Law and Democracy. – In: *Cambridge Polity Press*, 1996, pp. 44 – 45.
182. **Habermas**, J. The theory of communicative action. Boston, Beacom Press, 1989.
183. **Hamel**, G., C. K. **Prahalad**. Competing for the Future. Boston, Harvard Business School Press, 1994.
184. **Hamel**, G., C. K. **Prahalad**. Strategic Intent. – In: *Harvard Business Review*, May – June 1989.
185. **Hamel**, G., C. K. **Prahalad.** The Core Competence of the Corporation. – In: *Harvard Business Review*, May – June 1990.
186. **Han**, J., M. **Kamber**. Data Mining: Concepts and Techniques, Morgan Kaufmann, 2001
187. **Handy**, Charles. The Age of Unreason, Hutchinson, London, 1989.
188. **Hart**, T. E-Government: The Next American Revolution, 2000.
189. **Hernon**, P., E. **Robert**. Public Service Guidelines: A Critique. – In: *Journal of Academic Librarianship*, Vol. 25, May 99, Issue 3, pp. 229 – 231.
190. **Heskett**, J. Managing in the Service Economy. Harvard Business School Press, Boston, 1986.
191. **Hickman**, C., M. **Silva**. Creating Excellence: Managing Corporate Culture, Strategy and Change in the New Age. Penguin Books, 1984.
192. **Hill**, R., R. **Dunbar**. Social Network Size in Humans. – In: *Human Nature*, Vol. 14, No. 1, 2002, pp. 53 – 72.
193. **Hirst**, P., M. **Norton**. Electronic Government. Information Technologies and the Citizen. United Kingdom Parliament Parliamentary Office of Science and Technology, 1998. http://www.parliament.uk/post/egov.htm http://libraryjournal.reviewsnews.com/index.asp?layout=articleArchive&articleId=CA267142&display=searchResults&stt=001
194. **Hogan**, Bernie, Juan-Antonio **Carrasco**, Barry **Wellman**. Visualizing Personal Networks: Working with Participant-Aided Sociograms. Field Methods 19 (2), May 2007, pp. 116 – 144.

195. **Huisman**, M., M. A. J. **Van Duijn**. Software for Social Network Analysis. – In: **Models** and Methods in Social Network Analysis. P. J. Carrington, J. Scott, & S. Wasserman (Editors). New York: Cambridge University Press, 2005, pp. 270 – 316.
196. **Ignatova**, E. Intellectual Competitiveness – Organization and Knowledge Management in the Library. – In: **Proceedings** of the International Seminar of SULSIT: Contemporary Dimensions of the European Educational and Scientific Space, Sofia, Za Bukvite – O Pismeneh, 2014, pp. 28 – 44 [Language: BG].
197. **Ignatova**, E. To rediscover the knowledge: communicational culture of the university library and the informatization of the education. – In: **Contemporary** strategies and innovations in the knowledge management. Sofia, Za Bukvite – O Pismeneh, 2014, pp. 88 – 95 [Language: BG].
198. **Inclusion** in the Information Economy: Reframing the Debate. Available at: http://www.athenaalliance.org/apapers/inclusion.html
199. **Information** Skills in Higher Education: A SCONUL Position Paper. Available at: http://www.sconul.ac.uk/groups/information_literacy/papers/Seven_pillars.html
200. **Isenberg**, Daniel. How managers think. – In: *Harvard Business Review*, November – December 1984.
201. **Isenberg,** Daniel. Strategic Opportunism: Managing under uncertainty. Boston, Harvard Graduate School of Business, January 1986.
202. **Jabbra**, J., O. **Dwivedi**. Globalization, Governance, and Administrative Culture. – In: *International Journal of Public Administration*, Vol. 27, 2004, Issue 13/14, pp. 1101 – 1127.
203. **Jackson**, Matthew O. A Strategic Model of Social and Economic Networks. – In: *Journal of Economic Theory* 71, 2003, pp. 44 – 74.
204. **Jarillo**, J. Carlos. Strategic Networks: Creating borderless organizations. Butterworth-Heinemann, Oxford, 1993.
205. **Johansson**, V. Public libraries as democratic intermediaries: some example from Sweden. – In: *New Library World*, Vol. 105, 2004, Issue 1/2, pp. 47 – 59.
206. **Jreisat**, J. Governance in a Globalizing World. – In: *International Journal of Public Administration*, Vol. 27, 2004, Issue 13/14, pp. 1003 – 1029.

207. **Juran**, J. M. Juran on Quality Free Press. New York, 1992.
208. **Kearney**, A. T. Total Quality Management: A business process perspective. Kearney Pree Inc, 1992.
209. **Kim** and **Mauborgne**. Blue Ocean Strategy. Harvard Business Press. 2005
210. **Klir**, George J. Where do we stand on measures of incertainty, ambiguity, fuzziness, and the like? Fuzzy Sets and Systems, 24, 1987.
211. **Klir**, George J., Tina A. **Folger**. Fuzzy Sets Uncertainty and Information. NJ: Prentice-Hall, 1988.
212. **Krause**, M. Information Security Management Handbook. Auerbach Pub,2007.
213. **Limb**, A. Life-changing learning. – In: *Public Library Journal*, Vol. 18, Winter 2003, Issue 4, pp.78 – 79.
214. **Lin**, S. Nan, Burt **Ronald**, Karen **Cook**, eds. Social Capital: Theory and Research. New York: Aldine de Gruyter, 2001.
215. **Lindblom**, Charles E. The Science of Muddling Through. – In: *Public Administration Review*, Vol. 19, 1959, No 2.
216. **Linton**, Freeman. The Development of Social Network Analysis. Vancouver: Empirical Press, 2006.
217. **Luce**, R. E. Library Leadership and Local Politics: The Ins and Outs. – In: **Colorado** Libraries, 1988, pp. 11 – 13.
218. **Manski**, Charles F. Economic Analysis of Social Interactions. – In: *Journal of Economic Perspectives* 14: 2000, pp. 115 – 136.
219. **Markides**, Constantinos. A dynamic view of strategy. – In: *Sloan Management Review*, vol 40, spring 1999, pp. 55 – 63.
220. **Mason**, M. G. Politics and the Public Library: A Management Guide. – In: *Library Journal*, March, 1989, № 3, pp. 27 – 32.
221. **Melnick**, Jeff. Netwrix Blog. Top 10 Most Common Types of Cyber Attacks. [Online], 15 may 2018, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Denial-of-service%20(DoS)%20and%20distributed%20denial-of-service%20(DDoS)%20attacks.
222. **Metz**, Cade. Media players. – In: *PC Magazine* (USA), January 29, 2002, pp. 98 – 107.
223. **Miele**, T., N. **Welch**. Libraries as information centers for economic development. – In: *Public Libraries*, Vol. 34, 1995, No. 1, pp. 18 – 22.

224. **Minkel**, W. Who Owns e-Information. – In: *School Library Journal*, Vol. 46, Dec 2000, Issue 12, p. 43.
225. **Mintzberg**, H., B., **Ahlstrand**, J. **Lampel**. Strategy Safari: A Guided Tour Through the Wilds of Strategic Management. The Free Press, New York, 1998.
226. **Mintzberg**, Henry, J. B. **Quinn**. The Strategy Process. Prentice-Hall, Harlow, 1988.
227. **Mintzberg**, Henry. Crafting Strategy. – In: *Harvard Business Review*, July – August 1987.
228. **Mintzberg**, Henry. The Nature of Managerial Work. Harper and Roe. New York, 1973, p. 38.
229. **Moncrieff**, J. Is strategy making a difference? – In: *Long Range Planning Review*, vol. 32, No 2, pp. 273 – 276.
230. **Moody**, James, Douglas R. **White**. Structural Cohesion and Embeddedness: A Hierarchical Concept of Social Groups. – In: *American Sociological Review* 68 (1): 2003, pp. 103 – 127.
231. **Moore**, H. Mark Creating Public Value: Strategic Management in Government. Cambridge: Harvard University Press, 1995.
232. **Moore**, J. Predators and Prey. – In: *Harvard Business Review*, Vol. 71, May – June, pp. 75 – 86, 1993.
233. **Mulcaster**, W. R. Three Strategic Frameworks. – In: *Business Strategy Series*, Vol. 10, No 1, 2009, pp. 68 – 75.
234. **Mullins**, Nicholas. Theories and Theory Groups in Contemporary American Sociology. New York: Harper and Row, 1973.
235. **Nadel**, S. F. The Theory of Social Structure. London: Cohen and West, 1957.
236. **Nag**, R., D. C. **Hambrick**, M. J. **Chen**. What is strategic management, really? Inductive derivation of a consensus definition of the field. – In: *Strategic Management Journal*, Volume 28, Issue 9, September 2007, pp. 935 – 955.
237. **Newman**, Mark. The Structure and Function of Complex Networks. – In: *SIAM Review* 56: 2003, pp. 167 – 256.
238. **Nohria**, Nitin, Robert **Eccles**. Networks in Organizations. Second ed. Boston: Harvard Business Press, 1992.
239. **Noluxolo**, Gcaza, Rossouw von **Solms**, J. C. Jansen van **Vuuren**. An Ontology for a National Cyber-Security Culture Environment. June 2015.
240. **Noluxolo,** Gcaza, Rossouw von **Solms**, Marthie **Grobler**, J. C.

Jansen van **Vuuren**. A general morphological analysis: Delineating a cyber-security culture, 2017.

241. **Nooy**, Wouter, A. **Mrvar**, Vladimir **Batagelj**. Exploratory Social Network Analysis with Pajek. Cambridge: Cambridge University Press, 2005.
242. **Ohmae**, K. The Mind of the Strategist. McGraw Hill. New York, 1982.
243. **On demand** Government. 2003. – In: *IBM Business Consulting Series*, www.ibm.com
244. **Paré**, R. E-democracy and E-government: How will these affect libraries? – In: **68th** IFLA Council and General Conference, Glasgow, Scotland, 2002, pp. 18 – 24.
245. **Pascale**, R., A. **Athos**. The Art of Japanese Management. London: Penguin, 1981.
246. **Pascale**, Richard. Managing on the Edge. Simon and Schuster, New York, 1990.
247. **Pavlova**, M., S. **Denchev**, K. **Bosakova**, B. **Tetevenska**. The image and trust in the university – key factors in enhancing learner's motivation. ICERI2018 Proceedings, pp. 576 – 579.
248. **Paul**, Annie Murphy. I Feel Your Pain. – In: *Forbes*, Vol. 174, No. 13, Dec. 27, 2004.
249. **Peters**, T., N. **Austin**. A Passion for Excellence. Random House, New York, (also Warner Books), 1985.
250. **Peters**, T., R. **Waterman**. In Search of Excellence. Harper&Collins, New York, 1982.
251. **Peteva**, I. The right to information and information competence in modern social environment. Guide for information competency. Sofia: WINI-1837, 2009, pp. 21 – 26 [Language: BG].
252. **Peteva**, I. The informed citizen: transparency and security of information, Sofia, Za Bukvite – O Pismeneh, 2008. 196 p. [Language: BG].
253. **Pfleeger**, S. L., D. D. **Caputo**. Leveraging behavioral science to mitigate cyber security risk. – In: *Computers & Security*, Vol. 31, Elsevier Ltd, 2012, pp. 597 – 611.
254. **Pilkington**, Alan, Jack **Meredith**. The Evolution of the Intellectual Structure of Operations Management – 1980 – 2006: A Citation/Co-Citation Analysis. – In: *Journal of Operations Management*, 2009, Vol. 27, No. 3, pp. 185 – 202.

255. **Pine**, J., J. **Gilmore**. The Experience Economy. Harvard Business School Press, Boston, 1999.
256. **Pine**, J., J. **Gilmore**. The Four Faces of Mass Customization. – In: *Harvard Business Review*, Vol 75, No 1, Jan. – Feb. 1997.
257. **Popkin**, S. L., M. A. **Dimock**. Political Knowledge and Citizen Competence. – In: **C I t I z e n** Competence and Democratic Institutions. Pennsylvania State Univ. Press, 1996, pp. 117 – 146.
258. **Probst**, Gilbert, S. **Raub**, K. **Romhardt**. Managing Knowledge. Wiley, London, 1999 (Exists also in other languages).
259. **PULMAN**, 2003. The PULMAN Guidelines. 2nd ed. February, 2003. [Online], http://www.pulmanweb.org/DGMs/section1/CitizenParticipation.htm
260. **Quinn**, J. B. Intelligent Enterprise. The Free Press, New York, 1992.
261. **Rachman**, Gideon. An undeclared war in cyberspace. – In: *The Financial Times*, October 4, 2010.
262. **Radcliffe-Brown**, A. R. On Social Structure. – In: *Journal of the Royal Anthropological Institute*, 70 (1940): 1 – 12.
263. **Rehfeld**, J. E. Alchemy of a Leader: Combining Western and Japanese Management skills to transform your company. John Whily & Sons, New York, 1994.
264. **Reichheld**, F. The Loyalty Effect. Harvard Business School Press, Boston, 1996.
265. **Resnick**, Paul. Filtering information on the Internet. (Look for the labels to decide if unknown sofware and World-Wide Web sites are safe and interesting.). – In: *Scientific American*, March 1997, pp. 54 – 56.
266. **Revise Infrastructure & IT systems 2006, Bulgaria**. [Online], www.idg.bg/events/2006/0316134551-Revise_Nikolay_Dilov.ppt
267. **Richard Chase**, F., Robert **Jacobs**, Nicholas **Aquilano**, et al. Operations Management for Competitive Advantage, 2001.
268. **Rogers**, M., O. **Norman**. Online Library in E-Government Bill. – In: *Library Journal*, Vol. 126, 2001, Issue 10, p. 17.
269. **Salem**, Jr., A. **Joseph**. Public and private sector interests in e-government: a look at the DOE's PubSCIENCE. – In: *Government Information Quarterly*, Vol. 20, Issue 1, 2003, p. 13.
270. **Schartz**, Peter. The Art of the Long View. Doubleday, New York, 1991.
271. **Schein**, E. Organizational Culture and Leadership. Jossey – Bass, 1997.

272. **Schlesinger**, L., J. **Heskett**. Customer Satisfaction is rooted in Employee Satisfaction. – In: *Harvard Business Review*, November – December 1991.
273. **Schoderbek**, P., C. **Schoderbek**, A. **Kefalas**. Management Systems: Conceptual Considerations. BPI/IRWIN, 1990.
274. **Schumacher**, E. F. Small is Beautiful: a Study of Economics as if People Mattered, ISBN 0-06-131778-0 (also ISBN 0-88179-169-5).
275. **Scott**, John. Social Network Analysis. London: Sage, 1991.
276. **Scott**, John. Social Network Analysis: A Handbook. 2nd Ed. Newberry Park, CA: Sage, 2000.
277. **Selznick**, Philip. Leadership in Administration: A Sociological Interpretation, Row, Peterson, Evanston II, 1957.
278. **Sewell**, C., P. **Brown**. Customers for Life. Doubleday Currency, New York, 1990.
279. **Shannon**, Cl. A Mathematical Theory of Communication. – In: *Bell System Technical Journal*, 1948, Vol. 27, pp. 379 – 423, 623 – 656.
280. **Shapiro**, C., H. **Varian**. Information Rules. Harvard Business School Press, Boston, 1999.
281. **Shishkin**, Philip. Genes and the Friends You Make. – In: *Wall Street Journal*, January 27, 2009, http://online.wsj.com/article/SB123302040874118079.html.
282. **Slovac**, P. Perceived Risk, Trust, and Democracy. – In: *Risk Analysis*, 13, 1992, pp. 675 – 682.
283. **Slywotzky**, A., D. **Morrison**, T. **Moser**, K. **Mundt**, J. **Quella**. Profit Patterns. Time Business (Random House), New York, 1999.
284. **Sowa**, J. F., J. A. **Zachman**. Extending and Formalizing the Framework for Information System Architecture. – In: *IBM System Journal*, vol. 31, 1992, № 3.
285. **Stedman**, D. Transformation not Automation: The e-government Challenge. Demos, London, 2001. [Online], www.demos.co.uk/catalogue/transformation_page103.aspx.
286. **Stevans**, Melissa. Cybersecurity Vs. Information Security: Is There a Difference? BITSIGHT the standart in SECURITY RATINGS. [Online], march 15, 2016, [Cited: септември 20, 2018], https://www.bitsighttech.com/blog/cybersecurity-vs-information-security.
287. **Stewart**, Thomas. Intellectual Capital. Nicholas Brealey, London, 1997 (also DoubleDay, New York, 1997).

288. **Stoyanova**, Diana, Elena **Savova**, Irena **Peteva**, Ralitsa **Yotova**. Academic Research Projects for Students Support And Motivation In University Information Environment. – In: **Proceedings** of ICERI2018 Conference 12 – 14th November 2018, Sevilla, Spain, 2018, pp. 9706 – 9709.
289. **Stoyanova**, Diana. Contemporary Approaches for Diffusion of Information, Knowledge and Hypotheses – An Innovative Model for Motivating University Students, Phd Students, Post-Doctoral Students and Young Scientists – In: **Proceedings** of ICERI2018 Conference 12 – 14th November 2018, Sevilla, Spain, 2018, pp. 9706 – 9709.
290. **Stoyanova**, Diana, Ralitsa **Yotova**, Tsvetelina **Varadinova**. Innovations and training: integration of international projects in the process of training in cultural heritage for young scientists, phd students and students. – In: **Proceedings** of 9th annual International Conference on Education and New Learning Technologies, 3 – 5 July, 2017 Barcelona (Spain), 2017, pp. 9285 – 9288.
291. **Strang**, David, Michael W. **Macy**. In Search of Excellence: Fads, Success Stories, and Adaptive Emulation. – In: *American Journal of Sociology*, Issue 1 Jul 2001, Vol. 107.
292. **Sveiby**, K. E. The New Organizational Wealth: Managing and measuring knowledge-based assets. Berrett-Koehler Publishers, San Francisco, 1997.
293. **The Digital** Divide: Understanding and Addressing the Challeng. Available at: http://www.nysfirm.org/documents/html/nysfirm_digital_divide.htm
294. **The E-Government** Imperative. [Online], http://www.oecd.org/dataoecd/60/60/2502539.pdf
295. **Thomson**, K. L., R. von **Solms**, L. **Louw**. Cultivating an organizational information security. – In: *Computer Fraud & Security*, No. 10, 2006, pp. 7 – 11.
296. **Toffler**, Alvin. Future Shock. Bantom Books, New York, 1970.
297. **Toffler**, Alvin. The Third Wave. Bantom Books, New York, 1980.
298. **Traverso**, D. Outsmarting Goliath. Bloomberg Press, Princeton, 2000.
299. **Trencheva**, T., S. **Denchev**. The University's R&D Institutes as a New Educational Approach. – In: **Proceedings** of the International Technology, Education and Development Conference, Madrid, Spain, March 2 – 4, 2015, pp. 951 – 957.

300. **Tsvetkova**, Elisaveta, Irena **Peteva**, Ivanka **Pavlova**. Attitude of Bulgarian Library Specialists Towards Use of Library Resources for Mobile Learning. – In: **Proceedings** of 11th annual International Conference of Education, Research and Innovation (ICERI): Meeting the Challenges of 21st Century Learning. 12th – 14th of November, 2018, Seville, Spain. Ed. by L. Gómez Chova, A. López Martínez, I. Candel Torresp. Seville: IATED Academy, 2018, pp. 838 – 842.
301. **U.S. Department** of Education Institute of Education Sciences: Classification of Instructional Programs (CIP). Retrieved on October 26, 2009 from http://nces.ed.gov/pubs2002/cip2000/occupationallookup6d.ASP ?CIP=52.0205
302. **Valente**, Thomas W. Network Models of the Diffusion of Innovations. Cresskill, NJ: Hampton Press, 1995.
303. **Walzer**, N., J. **Gruidi**. The role of small public libraries in community economic development. – In: *Illinois libraries*, 1996, No 1, pp. 50 – 56.
304. **Wasserman**, Stanley, Katherine **Faust**. Social Network Analysis: Methods and Applications. Cambridge: Cambridge University Press, 1994.
305. **Watkins**, Susan Cott. Social Networks. – In: **Encyclopedia** of Population. Rev. ed. Edited by Paul George Demeny and Geoffrey McNicoll. New York: Macmillan Reference, 2003, pp. 909 – 910.
306. **Watts**, Duncan J. Six Degrees: The Science of a Connected Age. W. W. Norton & Company, 2004.
307. **Watts**, Duncan J. Small Worlds: The Dynamics of Networks between Order and Randomness. Princeton: Princeton University Press, 2003.
308. **Wayne**, R. An overview of public access computer software management. – In: *Computers in Libraries*, June 2004, pp. 24 – 30.
309. **Weaver**, B. F. Library involvement in state government information policy development in the United State. 68th IFLA Council and General Conference. Glasgow, Scotland, August 18 – 24, 2002.
310. **Webb**, John. Managing licensed networked electronic resources in a university library. – In: *Information Technology and Libraries*, December 1998, pp. 198 – 206.
311. **Weerasinghe**, Sh. Revolution within the revolution: The Sri

Lankan attempt to bridge the digital divide through e-governance. – In: *International Information & Library Review*, Vol. 36, Dec 2004, Issue 4, p. 319 – 327.

312. **Weiner**, N. Cybernetics. MIT Press and Wiley, 1948.
313. **Wellman**, Barry. Physical Place and Cyber-Place: Changing Portals and the Rise of Networked Individualism. – In: *International Journal for Urban and Regional Research*, 25 (2), 2001, pp. 227 – 252.
314. **Wellman**, Barry, Stephen D. **Berkowitz**. Social Structures: A Network Approach. Cambridge: Cambridge University Press, 1998.
315. **White**, Harrison, Scott **Boorman**, Ronald **Breiger**. Social Structure from Multiple Networks: I Blockmodels of Roles and Positions. – In: *American Journal of Sociology*, 81, 1976, pp. 730 – 80.
316. **Wilson**, M. James. An historical perspective on Operations Management. – In: *Production and Inventory Management Journal*, 1995.
317. **Wilson**, T. D. The nonsense of 'knowledge management'. – In: *Information Research*, 8 (1), 2002, paper no. 144. Available at: http://InformationR.net/ir/8-1/paper144.html
318. **Woo**, Hyung-jin. The hacker mentality: exploring the relationship between psychological variables and hacking activities. Athens, Georgia: s.n., 2003.
319. **Woodhouse**, Edward J., David **Collingridge**. Incrementalism, Intelligent Trial-and-Error, and the Future of Political Decision Theory. – In: **Redner**, Harry, ed. An Heretical Heir of the Enlightenment: Politics, Policy and Science in the Work of Charles E. Limdblom, Boulder, C: Westview Press, 1993, p. 139.
320. **Young**, H. e-Government-put the user first. – In: *Library & Information Update*, Vol. 2, Oct 2003, Issue 10, p. 59.
321. **Yuh-Shihng**, Ch. The E-government Web Promotion Strategies Based upon the Technological Supporting and Information Requirements. – In: *Journal of Information, Communication & Library Science*, Vol. 10, Jun 2004, Issue 1 – 4, pp. 51 – 64.
322. **Zachman**, J. A. A Framework for Information System Architecture. – In: *IBM System Journal*, vol. 26, 1987, № 3.
323. **Zaleznik**, Abraham. Managers and Leaders: Are they different? – In: *Harvard Business Review*, May – June, 1977.
324. **Zaleznik**, Abraham. The Managerial Mistique. Harper and Row, New York, 1989.

325. **Zuboff**, Shoshana. In the Age of the Smart Machine. Basic Books. New York, 1988.
326. **е-Правителство** 2005. Доклад за състоянието и развитието на електронното правителство в България. София: КЦИКУТ, 2005. Достъпно на: http://www.ccit.government.bg//common/documents/RetriveDocument.aspx?DocID=356&LanguageID=1

Интернет ресурси

327. http://apps.myspace.com/index.cfm?fuseaction=apps.main 05.2010 г.
328. http://bg.wikipedia.org/wiki/MySpace 04.2010 г.
329. http://blog.facebook.com/blog.php?post=190423927130 03.2010 г.
330. http://blog.twitter.com/2010/05/twitter-platform.html 05.2010 г.
331. http://conferences.alia.org.au/alia2000/proceedings/brian.hawkins.html
332. http://crossword.crozzword.com/blog/50-ideas-on-using-twitter-for-business-522/0 6.2010 г.
333. http://en.wikipedia.org/wiki/Application_programming_interface 06.2010 г.
334. http://en.wikipedia.org/wiki/Brad_Greenspan 04.2010 г.
335. http://en.wikipedia.org/wiki/Chris_DeWolfe 04.2010 г.
336. http://en.wikipedia.org/wiki/Criticism_of_Facebook 04.2010 г.
337. http://en.wikipedia.org/wiki/Facebook 04.2010 г.
338. http://en.wikipedia.org/wiki/Hacker_Croll 06.2010 г.
339. http://en.wikipedia.org/wiki/MySpace 04.2010 г.
340. http://en.wikipedia.org/wiki/Myspace#History 06.2010 г.
341. http://en.wikipedia.org/wiki/Open_Social 04.2010 г.
342. http://en.wikipedia.org/wiki/Ruby_on_Rails 06.2010 г.
343. http://en.wikipedia.org/wiki/Tom_Anderson_(MySpace) 04.2010 г.
344. http://en.wikipedia.org/wiki/Twitter#History 06.2010 г.
345. http://e-ukraine.org.ua
346. http://itbusiness.ca/index.asp?theaction=61&lid=1&sid=50751
347. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html 03.2010 г.
348. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html 04.2010 г.
349. http://konspiracy.assault.free.fr/blog/wp-content/uploads/Facebook-is-a-drug.jpg 05. 2010 г.
350. http://mediakomm.difu.de/en/index.php

351. http://notrial.info/news/it/2457.html 04.2010 г.
352. http://personalweb.about.com/od/myspacecom/a/whatismyspace_5.htm 06.2010 г.
353. http://techcrunch.com/2009/01/22/facebook-now-nearly-twice-the-size-of-myspace-worldwide/ 05.2010 г.
354. http://www.allfacebook.com/ 06.2010 г.
355. http://www.answers.com/topic/chris-dewolfe 04.2010 г.
356. http://www.answers.com/topic/tom-anderson-myspace 04.2010 г.
357. http://www.businessweek.com/technology/content/mar2006/tc20060327_215976.htm 05.2010 г.
358. http://www.cbc.ca/technology/story/2009/09/16/tech-facebook-300-million-users.html 05.2010 г.
359. http://www.cbc.ca/technology/story/2009/09/16/tech-facebook-300-million-users.html 04.2010 г.
360. http://www.ccit.government.bg/common/documents/RetriveDocument.aspx?DocID=328&LanguageID=1
361. http://www.checkfacebook.com/ 04.2010 г.
362. http://www.cilip.org.uk/default.cilip
363. http://www.computer.org/portal/web/csdl/doi/10.1109/MIC.2007.138 04.2010 г.
364. http://www.comscore.com/Press_Events/Press_Releases/2007/07/Social_Networking_Goes_Global/(language)/eng-US 05.2010 г.
365. http://www.econ.jhu.edu/pdf/papers/WP529harrington.pdf 03.2010 г.
366. http://www.egov4all.org/
367. http://www.facebook.com/petsociety
368. http://www.facebook.com/press/info.php?statistics 06.2010 г.
369. http://www.ft.com/cms/s/743f63c6-bea1-11de-b4ab-00144feab49a,Authorised=false.html?_i_location=http://www.ft.com/cms/s/0/743f63c6-bea1-11de-b4ab-00144feab49a.html&_i_referer= 05.2010 г.
370. http://www.gamezebo.com/news/2010/03/24/social-games-us-and-asia-why-looks-deceive 04.2010 г.
371. http://www.gis.com/
372. http://www.gsm.bg/articles/single/?ID=13860 04.2010 г.
373. http://www.insidefacebook.com/about/ 04.2010 г.
374. http://www.insidefacebook.com/facebook-global-market-monitor/ 04.2010 г.

375. http://www.jaiku.com/ 03.2010 г.
376. http://www.mmg.tu-sofia.bg/
377. http://www.oecd.org/dataoecd/60/60/2502539.pdf
378. http://www.public-libraries.net/html/new_technologies.html

Стоян Денчев

ИНФОРМАЦИЯ И СИГУРНОСТ

Българска
Първо издание

Рецензенти
проф. д.н. Ирена Петева,
проф. д.н. Стефан Симеонов,
проф. д-р Стефан Мичев

Редактор
Жана Ганчева

Художник
Павел Митков

Предпечат
БПС ООД

Академично издателство „За буквите – О писменехь“

ISBN 978-619-185-369-4 – pdf

Стоян Денчев е роден в гр. Елхово, България. Професор в професионално направление „Обществени комуникации и информационни науки“. Специалист по „Системен анализ“, „Информационен мениджмънт“, „Политически мениджмънт“, „Корпоративни комуникации“ и „Национална сигурност“. Доктор на науките.

Професионалното си развитие започва през 1978 г. в Централния машиностроителен институт в гр. София. По-късно работи като зам.-генерален директор в Информационния център за трансфер на технологии ИНФОРМА. Бил е Главен секретар на Министерския съвет, народен представител в 37-ото Народно събрание и посланик във Финландия. Създател и дългогодишен Ректор на Университета по библиотекознание и информационни технологии, гр. София. В настоящия момент проф. Денчев е директор на Научноизследователския институт по информация и сигурност.

Стоян Денчев завършва висше образование в СУ „Св. Климент Охридски“, Факултет по математика и механика, със специалност „Основи на кибернетиката и теория на управлението“. Специализира в Япония, Русия и Германия. Работил е като гост професор в Калифорнийският университет в Бъркли, САЩ.

Има над 220 публикации в областта на информационния мениджмънт, автоматизираните системи за обработка на информация и управление, бизнес и административните комуникации, националната сигурност и др. Негови книги, монографии и учебници се намират в най-големите световни библиотеки.

Членува в много национални и международни научни и обществени организации.