Глава 8.

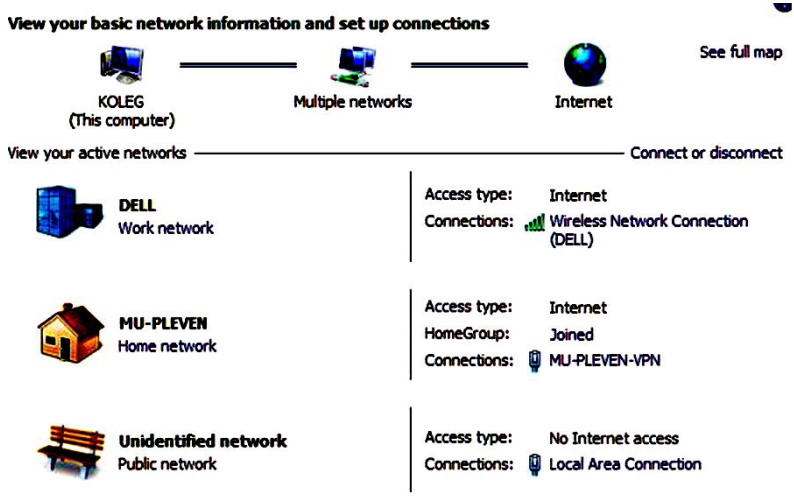
УСЛУГИ НА КОМПЮТЪРНИТЕ МРЕЖИ

Услуги на мрежите са редица дейности, свързани в повече от случаите с трансфер на файлове и файлови структури. Това могат да бъдат също справки в Интернет пространството или пък търсене на информация с обмен на аудио и видео данни в реално време. Отдалеченото управление на компютри с цел реализиране на конкретни настройки и достъп до общи информационни ресурси и устройства са пак типични услуги на компютърните мрежи. Основен дял в услугите на мрежите представлява и достъпът до Интернет базирани данни на институции, в това число държавни структури, университети, лечебни заведения, банки и други. Тъй като мрежите условно бяха разделени на два основни класа – локални и глобални, то и услугите които се ползват от тях също могат да бъдат разгледани отделно.

Услуги, използвани в локалните мрежи са онези, които могат да се реализират в рамките на една LAN мрежа. Те не предвиждат наличието на домейн в Интернет и могат да се ограничат в рамките на вътрешните IP адреси. Какви точно дейности и с какви средства могат да се реализират те в рамките на една локална мрежа много зависи и от нейната организация. В централизираните мрежи услугите са едни, а в разпределените (равноправните) те са други. При това голяма част от услугите, които се реализират в локалната мрежа са възможни и в рамките на глобалните мрежи. За да се използват услугите на компютърната мрежа е необходимо да се направят и съответните настройки. Всички настройки са достъпни от контролния панел и иконата за достъп до мрежата.

На фиг. 28 е показан един пример, при който са реализирани няколко връзки и съответно конфигурирани няколко различни мрежи. Първата мрежа е с безжичен достъп (Wireless Network

Connection). Тя е осъществила връзка с Интернет през точка за достъп с име (*Dell*). Статуса на тази мрежа по отношение на нейната защита е конфигуриран като *Work Network*. Втората мрежа е реализирана посредством VPN, чрез която е осъществена връзка с локалната мрежа на Медицински университет – Плевен. Идентификатора на тази мрежа е *MU-PLEVEN-VPN*, а статуса на нейната защита е *Home Network*. Третата мрежа от фигурата е локална (*Local Area Conection*) и тя е осъществена с помощта на UTP кабели и мрежови LAN карти на компютрите. Статуса на тази мрежа по отношение на нейната защита е *Public Network*.



Фиг. 28. *Мрежов достъп до информационни ресурси.*

В практиката рядко ще се наложи да се правят толкова мрежи и тук те са показани повече с учебна цел. Най-често се прави една връзка и ако потребителят разполага с безжичен рутер, и компютър с Wireless LAN карта, то това ще бъде безжичната *Wireless Network Connection*. При ползване услугите и на друга териториално отдалечена локална мрежа по технологията VPN, то в случая ще се направи и тази връзка. Третата с мрежовите карти може да бъде предпочитан вариант, ако компютърът е ста-

ционарен десктоп или пък се изискват високи скорости, които безжичната връзка не може да осигури.

За всяка една реализирана мрежа, която прави достъп до Интернет е нужно да се избере статус (вид) на мрежата. Чрез него операционната система автоматично ще определи степента на защита на информацията и ще направи съответните настройки. Възможни са три различни статуса и те са показани в примера.

Изборът на работна мрежа *Work Network* се използва при работа с малки служебни мрежи в рамките на един офис или едно работно място. При тази настройка не е възможно да се създават домашни групи или пък да се осъществява присъединяване към тях. Степента на защита, осигурявана от Windows се установява автоматично за този режим и е доста добра.

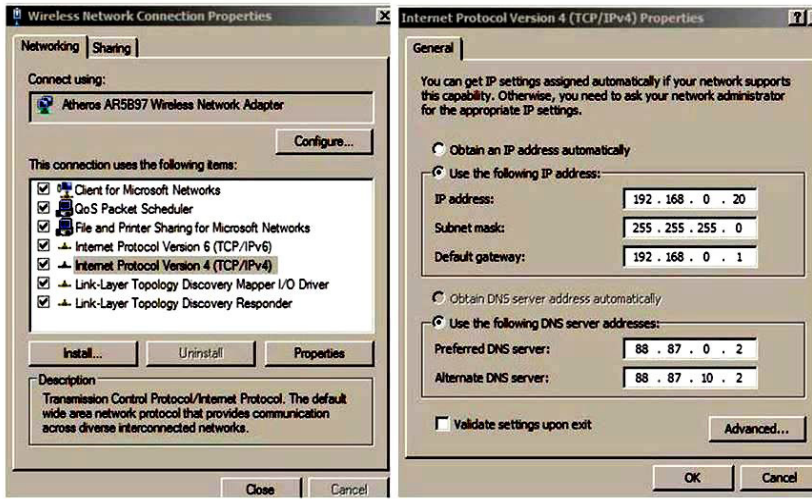
Домашна мрежа – *Home network* се използва за мрежи, при които включените компютри и потребителите са добре известни и на тях може да се има доверие. Компютрите в конфигурирана домашна мрежа могат да принадлежат и към домашна група. При условие, че в процеса на работа се налага често да се да се споделят файлове, то избора на *Home network* е може би най-добрия вариант.

Избор на Публична мрежа – *Public Network* е целесъобразно при работа с мобилни компютри, които често се използват на обществени места, като кафенета, летища, училища и други. Автоматично установените настройки при избора на тази мрежа няма да допуснат компютърът да бъде видим от други компютри. Настройката позволява и добра защита на локалния компютър от вируси, разпространявани чрез Интернет мрежата. Изборът на тази настройка е целесъобразен при директно осъществен достъп до Интернет, например посредством широколентова връзка или пък безжично чрез Wi-Fi. При попадане в безжично покритие и осигуряване на връзка с него, операционната система автоматично ще поиска избор на статус на мрежата.

Промяната на избраната мрежа може да стане по всяко време. За целта просто трябва да се отвори контролния панел и да се избере иконата за мрежата. От отворения прозорец (Фиг. 28) следва да

се избере съответната мрежа и да се смени статуса със желания. В практиката най-често се използва *Public Network* (Публична мрежа).

Освен избора за статус на мрежата в практиката доста често се налага да се установяват и други настройки и контроли. Това най-често са настройки, свързани с отделните устройства в мрежата и с техните IP адреси. Достъпът до тях може да се осъществи от команда *Properties* за избраната мрежа. Подобен пример е показан на фиг. 29, където са изобразени два диалогови прозореца. Този в ляво на фигурата предлага две страници с редица опции и настройки. Например чрез страницата *Networking* може да се определи дали да се даде разрешение за споделянето на файлове и принтери. Ако това трябва да е така, то опцията *File and Printer Sharing for Microsoft Networks* от тази страница трябва да е включена, така както е показано на фигурата. В практиката това е най-често срещания случай и означава, че потребителят ще може да споделя файлове и устройства в мрежата и с други клиенти свързани към нея.



Фиг. 29. *Настройки параметрите на компютърна мрежа.*

Прозорецът със страницата *General*, показан в дясно на фиг. 29 се отваря след избора на Интернет протокол *TCP/IPv4* и активиране на бутон *Properties*. Посредством него е възможно да се настроят IP адресите, чрез които конкретният компютър комуникира с другите устройства в локалната мрежа и в Интернет. Възможни са две основни категории настройки.

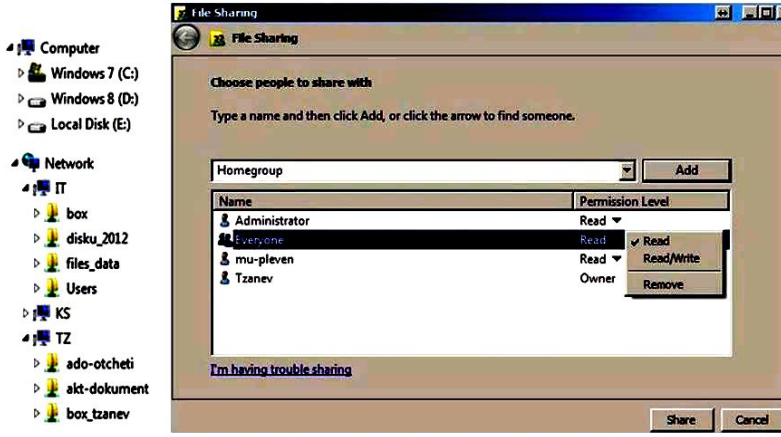
При първата (показана на фиг. 29) са включени опциите *Use the following IP address:* и *Use the following DNS server address:*. Това означава, че адресите на мрежата ще бъдат статично зададени. В този случай потребителят следва ръчно да въведе IP адресите, които са планирани за този компютър от администратора на мрежата. В примера са показани статичният адрес на компютъра, който е установен на 192.168.0.20, подмрежовата маска, която почти винаги в практиката за локалните мрежи е 255.255.255.0 и адресът на шлюза (*Default gateway*), през който се осъществява връзката с Интернет. Обикновено в практиката адреса на шлюза е компютърът с адрес 1 в същата мрежа, както е в примера, но може да има и отклонение от това правило, т.е. да е някакъв друг. В долните две полета на страница *General* се въвеждат статичните адреси на сървъра за преобразуване на логическите адреси DNS. Това може да бъде само един адрес, или един основен и един алтернативен. В примера това са адресите 88.87.0.2 и 88.87.10.2, които са предоставени и се поддържат от администратора на услугата. Задаването на статични адреси по показания тук начин е задължително, ако услугата го налага. В противен случай това не е нужно, а дори и не е за препоръчване.

При втората категория настройки (фиг. 29) трябва да са включат опциите *Obtain an IP address automatically* и *„Obtain DNS server automatically“* от страницата *General*. В този случай адресите, които ще се установяват за този компютър са динамични. Те ще се задават в определения диапазон автоматично от DHCP сървъра (например на безжичния рутер) и потребителят няма отношение към тях. Почти винаги в практиката, ако не се използват услуги изрично налагащи статични адреси, се използва тази настройка за мрежата.

Освен разгледаните по-горе настройки в една локална мрежа са налице и други. Те са достъпни от елементите посочени по-горе, но не са толкова често използвани и рядко се налага на потребителите да боравят с тях. Ако все пак се налагат някакви промени, то те ще бъдат свързани с конкретната услуга на мрежата, която ще трябва да се ползва от възможностите предлагани от мрежите.

В общия случай най-широко използваните услуги в рамките на една локална мрежа са обмен на файлове и файлови структури. Често се използва и услугата споделяне на мрежов принтер. В практиката се използват и услуги свързани със стартиране на програми върху отдалечен компютър, споделяне на устройства и други.

Обмен на файлове и файлови структури (директории) е най-често използваната услуга на локалната мрежа. За да се използва тя е необходимо първо мрежата да бъде настроена и в настройките да е указано тя да е достъпна за тези операции. Ако това е направено, то следващата стъпка е да се укаже споделяне (шерване) на съответния информационен ресурс. Това е елементарна операция и предвижда от контекстното меню за избрана директория или логическо устройство да се стартира команда *Share*.



Фиг. 30. *Споделяне на ресурси в състава на локална мрежа.*

Пример за използване на услугата споделяне е показан на Фиг. 30. Вляво на тази фигурата е изобразена част от дървовидната структура, която стандартно се извежда от Windows Explorer. В нея се изобразяват локалните ресурси на компютъра, включени в състава на иконата *Computer*. В примера това са трите логически устройства (C:), (D:) и (E:), върху които са разположени локалните информационни ресурси (файлове и директории) на локалния компютър.

Непосредствено под локалните устройства са изобразени онези ресурси, които са достъпните, чрез услугите на локалната мрежа. Те са включени в състава на иконата *Network* и в примера това са компютри с имена *IT, KS* и *TZ*. За всеки един от достъпните в мрежата компютри са изобразени и директориите, които са дефинирани като споделен ресурс. За компютъра *IT* това са четири директории, а за *TZ* те са три. Ресурсите, разположени на компютъра *KS* не са изобразени или пък върху него няма предоставени такива за достъп от други потребители на локалната мрежа.

Споделените ресурси в мрежата *Network* принадлежат на конкретния компютър, като правата за достъп до тях могат да бъдат за четене (*Read*) или пък едновременно за четене и запис (*Read/Write*). За да се сподели произволен ресурс (директория) от кой да е компютър в мрежата е необходимо той да се избере от дървовидната структура на локалния компютър (*Computer*), след което от контекстното меню да се стартира командата *Share With* и от там да се активира *Specific people*. Изпълнението на тази последователност от команди ще доведе до отваряне на прозореца *File Sharing*, така както е показано на Фиг. 30 в дясно. От него, чрез бутон *Add* следва да се избере потребителят (групата потребители), на който ще се предоставя (шерва) ресурса. В показания пример е избрана групата потребители, включени в *Homegroup*. След това трябва да се активира бутонът *Add*.

Възможни потребители, избирани посредством бутона *Add* могат да бъдат всички профили, които са създадени чрез операционната система на локалния компютър. Ако един потребител иска да има достъп до определен ресурс от повече различни ком-

пютри в мрежата, то той трябва да има създаден един и същи профил не само на собствения си компютър, а и на всички други в мрежата. В този случай той ще има достъп до споделения ресурс и от другите компютри.

Освен създадените профили за локалния компютър, предлагани чрез бутон *Add,* могат да се назначават права за достъп и за резервирани в операционната система потребители. Това са *Administrator* , *Guest*, *Everyone* и *Homegroup*. За всеки един от тях могат да се дефинират правата за четене или за четене/запис, както и самите те да се отстраняват от списъка чрез командата *Remove* от контекстното меню. В примера за шервания ресурс са добавени потребителят с профил *mu-pleven,* собственикът на компютъра с профил *Tzanev* и резервираните потребители *Administrator* и *Everyone.*

Резервираният потребител *Everyone,* за ресурса, за който е избран ще бъде достъпен за всички, които са свързани в мрежата. При споделяне на ресурси има и една особеност, която е свързана с профила, чрез който се работи в момента на локалния компютър. Този профил се означава с *Owner* в списъка с избраните потребители с определени права. За него не могат да се ограничават правата само за четене или пък за четене/запис. Той не може и да бъде изтрит от списъка с потребителите и винаги ще присъства в тях. В примера от Фиг. 30 в дясно, това е профилът (потребителя) с име *Tzanev*. За него правата върху конкретния ресурс са пълни, той е означен с *Owner* и не се предлага меню с възможностите за изтриване или дефиниране на конкретни права за достъп.

Използването на мрежов или споделен принтер е следващата по значимост услуга на мрежите. Тя се използва там където е организирана локална мрежа и в нейният състав има включени печатащи устройства. В този случай може да се създаде програмно-апаратна организация, при която всеки потребител на мрежата да може да използва принтера, определен като споделено или пък мрежово устройство. Принтерите могат да бъдат организирани по три основни начина – *локален принтер, споделен принтер и мрежов принтер*.

Локалният принтер се свързва директно към определен компютър, който е в мрежата или пък отделно от нея. Предимството на този вид печатащо устройство е, че то не изисква работеща локална мрежа и не зависи от други компютри, за да се реализира печат. Връзката между локалния принтер и компютъра най-често се осъществява чрез USB интерфейс или пък посредством безжична Wi-Fi връзка. На практика това зависи основно от възможностите на самия принтер, като много често са възможни и двата начина. Може да има и морално остарели принтери, които да използват паралелен порт или пък сериен порт. За да се използва локален принтер, освен апаратната връзка е необходимо да се осъществи инсталиране и на драйвер. Принтерите по принцип се продават със софтуер, в който са включени драйверите, а понякога и допълнителни програми за различни настройки. Инсталираното локално печатащо устройство е недостъпно за други потребители, които са абонати на локалната мрежа и не може да се използва от тях.

Споделен (шерван) принтер е вторият начин за използване на налично печатащо устройство. За да се реализира тази услуга е нужно към един от компютрите в мрежата да се конфигурира локален печат. Това може да стане като се изпълнят посочените по-горе указания. Ако принтерът вече е инсталиран като локален, то той може да бъде споделен с всеки потребител от същата мрежа. При това няма значение какъв е типът на принтера, достатъчно е той да е инсталиран на един от компютрите в мрежата. Всички други абонати на тази мрежа, с които принтерът е споделен, ще са в състояние да го използват за печат върху него. Процедурата по шерването на локалния принтер е елементарна. Тя предвижда от главното меню на операционна система Windows 7 да се избере командата *Devices and Printers*. Тя ще отвори диалогов прозорец, в който ще са изобразени локално инсталираните печатащи устройства. От там се избира желаното устройство, което ще се споделя и за него се активира контекстното меню. След това от това меню се стартира командата *Printer Properties* и от отворения диалогов прозорец се избира страницата *Sharing*. В нея са разположени инстру-

ментите за споделяне, които предвиждат активиране на опцията, която разрешава споделянето и избора на името, под което принтера ще бъде виждан, като споделено устройство в мрежата. След като се реализира тази процедура, то всеки потребител, за когото е разрешено може да използва този споделен принтер. Условието е той предварително да го е присъединил към групата на принтерите си *Devices and Printers*. Името на споделен принтер се предхожда от IP адреса или името на потребителя, който го е споделил – например \\Tzanev\Canon printer.

Предимствата на споделения принтер са преди всичко от икономическо естество, т.е. с едно печатащо устройство се обслужват няколко потребителя от мрежата. Освен икономията от печатащи устройства се премахва и нуждата от поддръжката на повече от едно устройство и се спестява от консумативите за тях.

Наред с предимствата са налице и определени недостатъци. На първо място това е необходимостта компютърът, към който е свързан споделеният принтер да бъде включен и принтерът да е в готовност за използване. Само при това условие може да се осъществи печат от потребителите на мрежата. Като недостатък може да се отчете и териториално отдалеченото място, където този принтерът се намира.

Мрежовият принтер е услуга, която може да бъде осъществена само, ако се разполага с устройство, което има възможности да я реализира. Тези устройства по принцип са обикновени принтери, в които има вградена мрежова карта за връзка към локална мрежа. Те имат възможност да се включат към произволна локална мрежа и да обслужват абонатите на тази мрежа. За тази цел е нужно мрежовият принтер да се свърже към локалната мрежа и да се направят необходимите върху него настройки. Това са настройки свързани с назначаване на IP адреса на принтера, определяне на неговото име, правата за достъп и други. Настройките се извършват чрез драйвера за конкретното печатащо устройство. Ако принтерът е инсталиран правилно, то използването му от потребителите е елементарно и е свързано с добавяне на мрежовия ресурс (в случай принтера)

към списъка на достъпните за съответния компютър печатащи устройства.

Използването на мрежов принтер има редица предимства спрямо споделения. Най-съществено от тях е, че не се налага да се ангажира компютър, който да изпълнява функциите на мрежов сървър и да е постоянно включен с готовност за работа. В случая е достатъчно само принтерът, който е в мрежата да бъде включен, да е зареден с хартия и да е в готовност за работа.

Недостатъците на мрежовия печат са по-високата цена на устройството, продиктувана от наличието на мрежови средства за връзка и управление. Териториално отдалеченото място от компютрите в рамките на мрежата е също един недостатък. Недостатък е и разпределянето на отпечатаните материали от различните клиенти в мрежата. Това обаче може да бъде преодоляно, ако се използва по-скъп мрежов принтер, който да има възможност да разпределя отпечатаните материали на отделните клиенти върху различни изходни тави (поставки). Тези устройства са доста по-скъпи от другите принтери.

Услуги, използвани в Интернет мрежите са разнообразните дейности свързани с информацията, нейния обмен, съхранение, защита и обработка. Голяма част от тези услуги са еднакво достъпни и изпълними, и в условията на локалната мрежа. Това означава, че услугите в Интернет мрежите могат да се разглеждат и като част от услугите на локалните компютърни мрежи.

В най-общ план услугите, които са специфични за Интернет мрежите са: Използване на информация от Интернет, посредством технологията на web страниците; Обмен на файлове, чрез ftp технологията; Използване на електронна поща по различните технологии за E-mail; Отдалечено използване на компютри и други:

Услугите базирани на Internet страниците или така наречените хипертекстови връзки са онези, чрез които потребителите имат възможност да се обръщат към домейн (сайт) с определен адрес. Сайтът е разположен (хостван) на някакъв компютър някъде по

света и има собствен уникален URL адрес. Обикновено при тази услуга всеки собственик на информацията предоставя една главна страница наречена „Уеб сайт“ (Web Site). Адресът на тази страница е публичен IP, той представя домейна на информационното съдържание и е резервиран в Интернет пространството. При това, вместо с физически IP адрес, той обикновено се представя с логически адрес, който пък се намира в списъка на именната система DNS. Самата услуга – WEB, често се записва пред URL адреса като WWW, което на практика е съкращение от World Wide Web, или това е технологията Интернет страници. Интернет страниците са услуги, които се базират на специални правила за обмен, нарични протоколи. За тази услуга най-често използваните протоколи са http: (Hyper Text Transport Protocol) и https. Те определят правилата и степента на сигурност, чрез която информацията се пренася от източника към приемника.

Протоколът http е създаден с цел обмен на информация в мрежата, която е в стандартен HTML (Hyper Text Markup Language) формат, т.е. форматът на данните за страниците в Интернет. Той показва начина, по който заявяващият компютър ще се свърже със сървъра и как точно ще се обмени информацията между тях. Имено този протокол е в основата на всички съвременни интернет страници, които се посещават от милиони и милиарди посетители. На практика това са правила, посредством които информацията от компютъра където е хостван сайта (web сървъра) се прехвърлят под формата на текст към този, който е заявил използването на тази страница.

Вторият протокол – https (Hyper Text Transport Protocol Security) има аналогично предназначение, само че прехвърлената посредством него информация е с много по-висока степен на защита. Тук към основния протокол се прибавя още един – SSL (Secure Sockets Layer). Неговото основно предназначение е да кодира заявените данни преди те бъдат изпратени към получателя. По този начини изпратената чрез https информация може да бъде захванатa и от други потребители, но тя няма да бъде разбираема за тях, за-

щото е кодирана. Използването на https изисква наличието на сертификати от специални сайтове и не всеки клиент може да използва кодиран по този начин сайт. Избраният сайт е сигурен ако притежава сертификат, издаден от лицензиран доставчик на услугата. Критерий, че това е така и има валиден сертификат е изобразения в горния ляв ъгъл на адресната лента на браузера малък катинар. Точно той показва, че посетеният сайт е сигурно защитен. Защитени сайтове ползват множество институции, като на първо място това са банки и финансови структури, където се извършват онлайн парични преводи или пък се борави с кредитни или дебитни карти.

В следващия пример е показано как може да се използва услугата web от конкретен сайт. Там се вижда, че адресът може да бъде записан по три различни начина. Този, който е най-вляво включва всички необходими елементи за адресиране на сайта. Примера в средата изключва спецификацията на протокола http, а този най-вдясно изключва и типът на услугата www. Записите имат следният вид:

http://www.dir.bg или **www.dir.bg** или **dir.bg**

Изключването на елементи от адреса на Интернет страницата е типичен случай в практиката и дори е препоръчителен. Ако те отсъстват, то браузерите ще ги поставят автоматично. Изписването на пълния адрес, обаче е гаранция, че той ще бъде открит, ако наистина съществува на някой Web сървър. Например често в практиката шифърът на услугата www е задължително да се пише и ако това е пропуснато, то браузърът няма да открие сайта.

При отваряне на страница в браузъра, често след адреса на сайта автоматично се поставя наклонена на дясно черта и след нея се изписва адресирана в този сайт страница. Тези адреси могат да бъдат много дълги и да са пълни с неразбираеми за потребителя символи. Всичко това са адреси, посочващи вътрешни за сайта страници. Подобен пример за директно адресиране на страница от конкретен сайт, може да изглежда по следният начин:

http://www.telnet.bg/?mod=faq#promotions.

В примера, веднага след името на домейна е поставена дясно наклонена черта и след нея е записан адрес на страница от този домейн. Адресът може да бъде въведен директно в адресната лента на браузера, като по този начин началната страница (Home page) на този сайт ще се прескочи и ще се направи директен достъп към посочената в адреса страница. В случая това е страница с много полезна информация за потребителите, която предлага регионалният кабелен Интернет оператор (ISP) Телнет на своите клиенти.

Услугите, базирани на файлов обмен в Интернет са следващите по приложение сред потребителите на глобалната мрежа. Чето те се наричат „FTP“ (File Transfer Protocol), като това е името на протокола за обмен на файлове. Протоколът е подобен на http, само че тук не се обменят HTML страници, а отделни файлове. Може да се каже, че ftp протокола е надстройка на TCP/IP и е предназначен за прехвърляне на различни файлове, включително и такива с много големи обеми. Прехвърлянето се осъществява между два компютъра, които са свързани в Интернет. При това компютрите могат да бъдат инсталирани с различни операционни системи, достатъчно е да имат връзка с Интернет. Услугата ftp е много подходяща за организации където се налага често прехвърляне на различни файлове. За този случай е целесъобразно файловете да се разположат върху един общ компютър и от там при нужда, чрез тази услуга де се прехвърлят към множеството други компютри, които са свързани към Интернет.

Технологията за обмен на файлове (ftp) работи по модела „клиент-сървър“ и се осъществява между централен обслужващ компютър, наречен „FTP сървър“ и приемащ компютър, наречен „FTP клиент“. В широката практика посоката на обмен на файловете почти винаги е от сървъра към клиента. Обратната връзка за предаване от клиента към сървъра е по-рядко осъществявана операция, а доста често тя е забранена и невъзможна.

За връзка с FTP сървъра се изисква програма, с която да се осъществява връзката и да се реализира обмена. Обикновено тази програма се нарича „ftp клиент“ и в практиката са налице може-

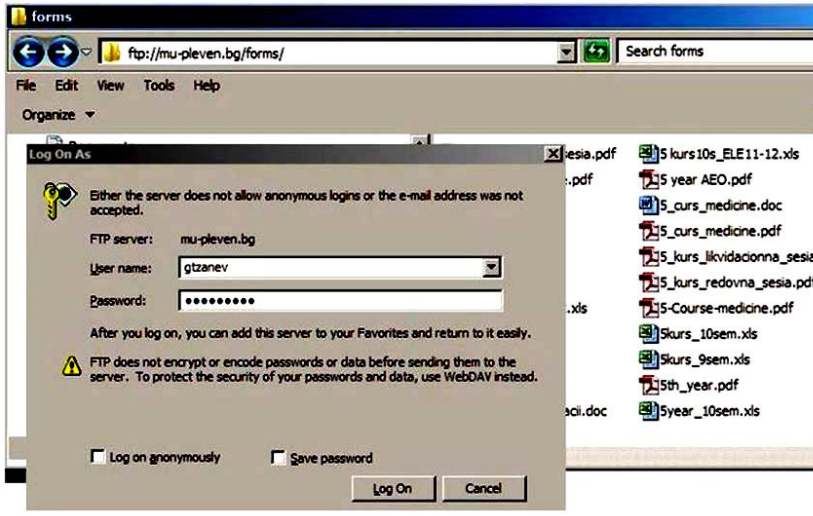
ство подобни. Такива например са програмата FileZilla (https://filezilla-project.org/), програмата SmartFTP (http://www.smartftp.com/) и много други. Работата с подобни програмни е сравнително лесна и предвижда разучаването на интерфейси и на няколко основни команди.

Освен специализираните програми за FTP услуги може да се използват и възможностите на Windows. Например посредством Windows Explorer може да се направи достъп до произволен ftp сървър. За тази цел е нужно в адресната лента на програмата да се въведе Интернет адреса на ftp сървъра. Особеното при въвеждане на такива адреси, е че пред името на домейна се поставя не http://, а шифърът на ftp услугата – ftp://. Например за достъп до ftp сървъра на МУ – Плевен трябва да се въведе ftp://mu-pleven.bg, а за достъп до този на Телнет ftp://telnet.bg и т.н. Почти всички по-големи организации и интернет доставчици предлагат ftp услуга.

Особеното при реализиране на FTP е, че сървъра винаги иска права за осъществяване на достъпа до неговите ресурси. Тези права трябва да се удостоверят от клиента с потребителско име и парола. За тази цел, веднага след въвеждане на валидния адрес до ftp сървъра, клиентската програма ще отвори диалогов прозорец. В него следва да се въведе името на потребителя и паролата за достъп.

На фиг. 31 е показано как чрез Windows Explorer може да се направи достъп до ftp сървъра на МУ – Плевен. В адресната лента е въведен адрес ftp://mu-pleven.bg/forms, като веднага след това програмната е предложила прозореца, в който се въвеждат името за достъп до сървъра (в примера gtzanev) и под него паролата. След въвеждане на правата за достъп ще се отвори прозорец, в който ще се изобрази съдържанието на избраната директория (в примера forms) от ftp сървъра. Работата с ftp клиентската програма на Window е много подходящ вариант за потребители, които нямат друга програма или пък не знаят как се работи с нея. Особеното при Windows Explorer е, че малко по-тромаво се работи с него. Например, там няма как да се види графически дървовидната структура на ftp сървъра и това трябва да става само с инструментите предлагани от

адресната лента. За прехвърляне на файлове, чрез Windows клиента е най-добре да се отворят два прозореца – единият на приемника, а другият на ftp сървъра. В този случай прехвърлянето на файловете се свежда до операция влачене между двата отворени прозореца.



Фиг. 31. *Достъп до валиден ftp сървър с дефинирани права.*

Освен контролирания достъп съществуват много ftp сървъри, които предлагат и свободен (anonymous) достъп за различни клиенти от Интернет пространството. Някои от тях са напълно свободни и не изискват въвеждането на каквито и да било данни за вход. Други пък поддържат анонимен достъп с фиктивно въведени права. При тях най-често параметрите на анонимния достъп са потребително име „guest“ и парола за ползване услугите на валиден за електронна поща електронен (E-mail) адрес.

Електронна поща (E-mail) е услуга, която вече се ползва може би от почти всички потребители, които имат достъп до компютри и до Интернет. Първоначално тя се е реализирала само при наличие на два свързани в определен момент компютъра, т.е. това

е ставало в реално време. Сега тази услуга не се осъществява по този начин и е независима от връзката в момента на изпращане или получаване на съобщението. При сегашната организация изпращача на съобщението го препраща към компютър, който изпълзява ролята на пощенски сървър (E-mail сървър). Този сървър винаги е свързан към Интернет, като приема, съхранява и изпраща по заявка електронните съобщения. За тази цел се използват специални правила за обмена на информацията, наричани E-mail протоколи. Един от най-често използваните протоколи за транспортиране на съобщенията от изпращача към пощенския сървър е SMTP (Simple Mail Transfer Protocol). Той използва преносната среда на Интернет и популярният TCP/IP протокол, над който се надстройва. Друг протокол, който се използва за прочитане на информацията от сървъра върху компютъра на клиента е POP3 (Post Office Protocol, version 3). Има и други протоколи, които се използват за транспортиране на електронните съобщения, но те не представляват интерес за широкия потребител.

По принцип електронната поща е директория върху някой компютър (E-mail сървър), който е свързан към Интернет. Върху този компютър е инсталирано програмно осигуряване, чрез което се реализират всички дейности по осигуряване на E-mail услугата. Достъпът до директорията на този компютър е възможен само от потребителят, на който са предоставени права за това.

Правата за достъп, както и при ftp услугата, се предоставят с потребителско име и парола. След като притежава тези права, собственикът на пощенската кутия има възможност да изпраща и да получава електронни съобщения. Електронните съобщения могат да бъдат текст, изображения и прикачени към тях файлове.

Директорията (пощенската кутия) е с фиксиран капацитет, който се определя от администратора на E-mail сървъра. Този капацитет за различните пощи е различен и често варира от порядъка на няколко или десетки гигабайта. Получените на сървъра електронни съобщения могат да се съхраняват много дълго време или пък да се изтриват след като клиента ги е получил. Те могат да се изтриват и

от лицата, които администрират сървъра. Съществува възможност и клиента на пощенката кутия сам да определя кое съобщение да бъде изтрито и кое да се запази за дълго време.

За да се използва електронна поща е необходимо да се регистрира електронен (E-mail) адрес. Този адрес се състои от две основни части, разделени със символа **@** и има следният вид:

ime-potrebitel@URL, пример: – **univesitet@dir.bg**

Първата част на адреса представлява име на потребителя – user name (ime-potrebitel). То се избира и назначава от клиента при регистрирането на пощенската услуга. Името трябва да бъде уникално за пощенския сървър и да не се повтаря с друго на същия сървър. Освен това при избора на име не всички символи са разрешени, като различните регистратори, често налагат различни ограничения.

Като общо валидно за всички регистратори могат да се посочат изискванията адреса задължително да започва с буква и да съдържа само латински букви. Допустими са също цифрите от 0 до 9 и някои специални символи като тире (-), долна подчертаваща (_) и точка (.). В някои случаи са допустими и други специални символи, но препоръката е да не се прибягва до тях, макар и да са разрешени. Освен това често имената на потребителя се ограничават по минимален и максимален брой на символите. Всички тези ограничения и правила се дефинират от администраторът на конкретната електронна поща и потребителите трябва да точно да ги спазват. Налице е и друг пример в практиката, когато исканото име за потребител вече е заето и не може да бъде ползвано от други. За да улеснят тази процедура, администраторите често поставят поле за проверка на желаното име, с което изборът става по-лесен и по-бърз. Препоръчва се при избора на името, потребителите да се ориентират към смислени имена, които да ориентират и да са сравнително лесни за използване, а не поредица от безсмислици, символи и цифри.

Втората част на адреса е пълното име на домейна, където е регистрирана пощата, т.е. URL адреса. Ако пощата е разположена на сървъра на институцията или организацията, то това ще бъде

техният собствен регистриран домейн, с който присъстват в Интернет – например mu-pleven.bg. Ако пък е електронна поща за обществено ползване и със свободен достъп, то името на домейна ще бъде това, което е на собственика на услугата, например dir.bg, abv.bg и т.н.

В зависимост от това къде е регистрирана електронната поща и по какъв начин се използва тя, в практиката условно могат да се разграничат два типа пощи – локални и глобални. Наименованията са условни, но разликата между двете са съществени. За всяка една от тях са налице определени особености и правила за работа.

Локалната поща е онази, която е разположена върху собствения сървър на организацията или пък на директния Интернет доставчик. Тези пощи налагат използването на програми при потребителя, които се наричат пощенски клиент. Какъв точно пощенски клиент ще се използва зависи от администратора на услугата. При локалните пощи най-често се използва протокола POP3 или подобния на него, но доста по-усъвършенстван IMAP (Internet Message Access Protocol). Всички съвременни програми за пощенски клиент поддържат тези протоколи. При локалните пощи с POP3 съобщенията се изтеглят от E-mail сървъра на локалния компютър на потребителя в директория поддържана от програмата пощенски клиент. Ако се използва IMAP протокола, то директорията и електронните съобщения в нея се пазят на сървъра. В този случай те се проверяват и отварят дистанционно чрез пощенския клиент на E-mail сървъра без да се изтеглят на личния компютър. При желание от страна на потребителя съобщенията могат и да се изтеглят на локалния компютър.

Предимствата на локалните пощи са много. На първо място името може да бъде избирано произволно от потребителя, чрез договорки с администратора. На второ място, е възможен и директен контакт с доставчика за моментно възникнали проблеми. Освен това информацията на собствения сървър може да бъде контролирана, да се архивира и по този начин да се повиши нейната степен на сигурност. Контролът на електронните съобщения при локални-

те пощи е изцяло от правомощията на администратора, който носи и отговорност за пощата. Не на последно място е и възможността тази поща да се договори с максимално необходимия за клиента капацитет.

Наред с предимствата са налице и определени недостатъци. Един от тях е недостатъчно добрата връзка, когато пощата се ползва извън пределите на организацията или в други страни по света. В някои от тези случаи е възможно потребителят на локалната поща дори да няма достъп до информацията в нея. Причината за това може да бъде и отсъствието на съответната програма „пощенски клиент“, с която би следвало да се направи достъпа. За потребители работещи с операционна система Windows и нейните различни версии този проблем рядко може да съществува. Това е така, защото в нея има интегриран сравнително универсален пощенски клиент и той е масово използваната програмата Outlook. Естествено в него трябва да се направят и съответните настройки за връзка с E-mail сървъра на организацията, но те са малко, лесно се заучават и прилагат.

Глобалните пощи са разположени в информационното пространство на големи Интернет доставчици с национално и международно значение. Често тези доставчици се наричат портали и те предлагат услугата електронна поща. Такива са например националният портал dir.bg, порталът за пощенски услуги abv.bg, порталът за търсене Google, който предлага услугата Gmail, порталът Yahoo, Hotmail и много други. Има и по-малки организации, които предоставят свободни глобални пощи, но те не са толкова популярни.

Глобалната поща се нарича още „уеб мейл“ (Web E-mail) и услугата, която се предлага от нея представлява базирана някъде в Интернет електронна поща. Чрез такава поща може да се четат и изпращат писма от всяка точка на света, без да има нужда от инсталирана програма от вида на някакъв пощенски клиент. На практика може да се счита, че глобалната поща е услуга, която се ползва през Интернет и не зависи от това какви програми има инсталирани на компютъра на потребителя. Единственото условие тук е той

да има някаква работеща операционна система, връзка с Интернет и инсталиран произволен браузер, с който да се обслужват сайтовете. Получаването и изпращането на електронни писма при уеб базираните електронни пощи се осъществява само чрез Интернет браузър, в това число Internet Explorer, Mozilla FireFox, Chrome, Opera и други.

Предимствата на глобалните пощи са, че в повечето случаи те са свободно достъпни за всички, които желаят да ги използват. Не изискват инсталирането на какъвто и да било друг софтуер, освен традиционно използвания от потребителя. Освен това сайтовете, чрез които те са достъпни предлагат и редица други информационни услуги. Като най-голямо предимство, обаче си остава възможността за достъп до електронните съобщения от произволно място по света, където има Интернет връзка.

Глобалните пощи имат и определени недостатъци. На първо място това е изборът на потребителско име. В някои от популярните уеб базирани пощи това се оказва проблем, защото желаното име е заето и трябва да се търсят алтернативи. Като недостатък може да се счита и фиксираният капацитет на пощенската кутия, макар че вече се предлагат достатъчно големи обеми. При глобалните пощи доставчика не носи никаква отговорност за информацията и връзката с него е почти невъзможна. Освен това често се случва той временно да преустановява достъпа до информацията от електронните съобщения. Сигурността на информацията при глобалните пощи е също проблем и това трябва да се има предвид от клиентите.

За използването на свободни уеб базирани пощи се използва процедура за регистриране, която се реализира от потребителя. Обема от дейности в нея се определя от собственика на услугата и предвижда попълване на информация за клиента. Това е информация свързана с потребителското име, парола за достъп и други данни, които за различните доставчици са различни. При попълването на регистрационните форми има задължителни и препоръчителни данни. Задължителните обикновено са отбелязани със звез-

да и потребителят трябва да ги попълни правилно, за да получи достъп до услугата.

Голямото разнообразие на предлагани свободни уеб базирани пощи прави доста труден избора за потребителя. Критериите, които следва да се използват са много, но като че ли един от тях е популярността на сайта. За страната може би най-популярния сайт е abv.bg, но с много голямо приложение е и порталът dir.bg. От международните доставчици към момента с най-голяма популярност са сайтовете на Google – gmail.com и на Майкрософт hotmail.com, или поне това сочи статистиката сега. Ако се направи една систематизация, то в най-общ план като ориентировъчни критерии за избор на конкретна уеб базирана електрона поща мога да се посочат:

– *Лесен и интуитивен потребителски интерфейс.* – Това означава, че отделните елементи са разположени правилно, достъпни са и са лесни за разбиране. Няма прекалено много и излишна информация. Рекламите предлагани със сайта са сравнително малко или дори отсъстват (рядко срещано в практиката);

– *Бърз достъп до информацията в пощата.* – Различните доставчици предлагат различна скорост за обслужване на пощите. При някои от тях самият сайт се зарежда бавно, а и достъпът до информацията в него не е с достатъчно добра скорост. Това особено силно се усеща при изпращането на информация с големи по обем файлове;

– *Голям обем на използваното дисково пространство.* – Този критерий е свързан с предлаганото дисково пространство на сървъра на доставчика. Различните доставчици предлагат различен обем, като най-често той е от порядъка на един до десетки гигабайта. За контрол на заетото пространство, обикновено доставчика извежда съобщение и то е в проценти от заетото пространство. В тези случаи потребителите следва сами да се грижат за свободното място и при необходимост да изриват ненужната вече информация. Липсата на контрол може да се окаже проблем при използването на пощата.

– *Голям обем на прикачените файлове.* – Различните доставчици допускат и различен обем на файловете, които могат да се прикачват към електронното съобщение. Какъв е точно обема,

следва да се търси в условията за използване на пощата, но най-често в практиката той варира от порядъка на 20-30 MB. За някои пощи при опит да се прикачи голям файл се извежда съобщение, веднага след като се избере опцията за прикачване. Има обаче и такива, при които не се извежда никакво съобщение и операцията по прехвърлянето на прикачения файл просто не се реализира. От практическа гледна точка не се препоръчва прикачване на големи файлове. Ако все пак това се налага, то най-добре е да се търсят други сайтове и други способи за обмен на файлове, а не прикачени към електронното съобщение.

– Сигурност на информацията и защита от вируси и СПАМ. – За повишаване сигурността на информацията доставчиците използват различни способи и антивирусни програми. Такива се прилагат и срещу получаването в пощата на нежелани съобщения. Те най-често представляват реклами, натрапчиви надписи или поредица от безсмислици и се наричат СПАМ. Доставчикът на услугата проверява съобщенията за СПАМ на базата на определени правила и ако прецени, че са такива ги фиксира като нежелани. Подобни съобщения не се записват в кутията с електронните съобщения, а се прехвърлят в специална директория, наричана СПАМ директория. Ако филтрите на информацията (проверките), прилагани от доставчика не са достатъчно надеждни, то може да се окаже, че действително електронно съобщение е попаднало в спам директорията и потребителят няма да го получи. Ето защо е препоръчително често да се преглежда и тази директория. Ако това не се прави, може да се окаже, че има загубени и непрочетени действително съобщения.

Могат да се посочат и други критерии при избора на доставчик за уеб мейл. Това са например наличието на разнообразни възможности за индивидуално настройване, възможност за известяване към мобилен телефон за получено ново електронно писмо и други.

От всичките посочени критерии, най-важният си остава сигурността на информацията. Потребителите следва да имат предвид, че независимо от това каква поща ползват – глобална или локална, то вероятността за изтичане на информация е голяма. Точно това

налага в практиката да се прилагат такива практики и правила, които свеждат до минимум възможността за загуба на информация.

Препоръки за работа с електронни пощи са набор от правила, които могат да се систематизират по определени признаци и да се отправят като послания към потребителите. Посредством тях възможностите за загуба на информация или пък приемане на нежелан софтуер могат да се сведат до минимум. Неспазването на определени правила може да доведе и до неправомерно изтичане на лична информация за клиента на пощенската услуга. Така например чрез електронната поща е възможно да се присвои пълният електронен адрес, заедно с потребителското име и паролата за достъп. По този начин, този който е попаднал на подобна информация може свободно да преглежда личната поща на потребителя и да сваля данни за него.

Способите за присвояване на електронен адрес са различни. Често използвания от тях е потребителят да бъде препращан директно към сайт, който на външен вид е подобен на интернет сайта на организацията, която предоставя услугата за електронна поща. В случая клиента без да подозира нищо, въвежда своите данни за достъп, но сайтът му отказва такъв, при което най-често последват още няколко опита. В същото време въведените от измамеият данни се копират и могат да се използват за достъп до неговата електронна поща. Този способ за присвояване на права за достъп до електронна поща се наричат Фишинг. Подобен фишинг способ се използва и от хора, които се представят от екипа за обслужване на електронната поща (администраторите). Те изпращат съобщения до потребителите с искане същите да изпратят данните си за достъп. Като причина за това обикновено се посочва установен нерегламентиран достъп до регистрацията, пропадане на информация и други. Нищо неподозиращият потребител си въвежда данните и те стават достояние, за онези които искат да проникнат в личната поща. За да се повиши сигурността при работа с електронни пощи и се намали вероятност за кражба на електронни адреси и потреби-

телска информация е задължително да се прилагат някои правила. *По-съществените правила за работа, които са лесно изпълними от всеки потребител са:*

1) Винаги трябва да се проверява адреса на Интернет сайта, който предоставя услугата, дали точно съответства на действителния. При каквото и да било съмнение, той трябва веднага да се затвори и да не се въвежда в него никаква информация. Понякога измамници регистрират сайт с име и дизайн много близки до тези на сайта на организацията. Това заблуждава потребителите и те влизайки в него със своите параметри за достъп на практика ги предоставят на други лица, разработили този сайт с користни цели.
2) Никога не бива да се изпращат лични данни за достъп в отговор на получено електронно съобщение с покана за това. Хората, с които потребителят редовно контактува не биха поискали да получат данните, чрез електронната поща.
3) Винаги след използване на услугата електронна поща, потребителят трябва да излиза от нея посредством специален инструмент. Този инструмент обикновено е с надпис „изход“ или нещо от този род, например оформен в графичния интерфейс бутон. Съветът е да се търси този инструмент и затварянето задължително да стане с него. Незатварянето на пощата може да бъде причина други да се възползват от нея и да снемат личните данни на собственика.
4) Паролите за достъп до пощенските услуги трябва да са надеждни, да не са свързани с рождени дати и ЕГН и да съдържат специални символи, като например $, !,&, @, # и други. Тези пароли не бива да бъдат постоянни, а периодично да се променят. Освен това трябва да се внимава с поканата за промяна на паролата от страна на доставчика. Доста често това е покана от този, който иска да отнеме

или присвои достъпа до пощата. Потребителите трябва да знаят, че всеки доставчик предлага средства те сами да си сменят паролата и никога няма да поиска тя да му бъде изпратена. Освен това са налице и инструменти за възстановяване на правата върху пощенска кутия, за която достъпът е отнет, например след забравена парола.

5) Личните данни за достъп до пощенската кутия, като парола и потребителско име не бива да се записват в общодостъпни файлове. Ако това се налага, то тези файлове трябва да имат надеждна защита срещу неправомерен достъп, т.е. да са защитени с парола.

6) За създаване на електронна поща с предоставяне на пълни данни за нея не бива да се използват услугите на други лица, без да се прочетат правилата, които доставчика изисква. Ако все пак това се налага, то паролата за достъп в никакъв случай не бива да се съобщава или веднага след това да се направи промяна от собственика.

7) В никакъв случай не бива да се отварят писма от съмнителни податели, и такива, за които се извеждат предупреждения от антивирусните програми. С тях е твърде вероятно да се запишат вирусни програми, който могат да следят за въвежданата от потребителя информация. Обикновено тези програми записват въведените от потребителя данни, като банкови сметки, потребителски имена, пароли за достъп до електронни пощи, до бази с данни и други подобни. В последствие данните се изпращат от вирусната програма до този, който я е изпратил и той ги използва за измамни цели.

При подготовката на електронните съобщения следва да се спазват и редица правила. Това са правила, които ще гарантират, че съобщението ще пристигне до получателя. Трябва да е ясно на всеки, че програмите, които приемат съобщенията ги проверяват и ако открият нещо подозрително, то веднага ги препращат към

СПАМ кутията. Тези програми се наричат СПАМ филтри и различните доставчици прилагат различни правила и ограничения на входящата електронна поща. Колкото по-надеждни и по-разнообразни са тези правила, толкова полученият спам в предназначената за него кутия е по-голям. Това обаче има две страни. Много често рестриктивните СПАМ филтри изпращат и качествените съобщения в СПАМ кутията. За да се избегне това и да се отговори на общоприетите принципи при подготовката на съобщенията трябва да се спазват определени правила. *По-съществените норми, които завишават антиспам защита на електронните съобщения са:*

1) Не бива да се използват прекалено много специалните символи и особено знак удивителна (!). Това често се контролира от СПАМ филтрите и не се допуска във входящата пощенска кутия. Най-често такива съобщения директно се прехвърлят към СПАМ кутията.

2) В текста на съобщенията не трябва да се съдържат много често думи в превъзходна степен, като „огромен“, „невероятна цена“, „купете веднага“ и други подобни. Те също са обект на филтриране и много често прехвърляне на съобщението в СПАМ директорията.

3) Ако текстът на съобщението е подготвен с Word или друга текстообработваща програма трябва да се има предвид, че в него освен полезната информация има и различни форматиращи символи. Тези символи може да се окажат обект на СПАМ филтрите. В подобен случай се препоръчва информацията да се копира в обикновен текстов редактор, например NotePad и от там да се прехвърли в полето на електронното съобщение. По този начин всички специални символи, които потребителите не виждат ще бъдат автоматично премахнати и те няма да бъдат обект на филтрите.

4) Не се препоръчва използването само на големи букви или пък на цели фрагменти и думи от тях, както и да се прилагат ярки цветни шрифтове. Това, от една страна се приема

като неучтиво (грубо и натрапчиво) водене на кореспонденцията и от друга може да са окаже предмет на филтриране и изпащане в СПАМ кутията.

Освен посочените по-горе общи препоръки при подготовката на електронните съобщения има и други, които е трудно да се систематизират под общ знаменател. Те се натрупват като опит в практиката при работата с пощите и квалифицираните потребители ги спазват.

Както при подготовката, така и при отварянето на прието пощенско съобщения са налице доста правила. Голямата част от тях са изпитани в практиката и потребителите следва да ги знаят и доколкото е възможно да ги *спазват. По-съществените правила при използване на електронни адреси и отваряне на съобщения тях са:*

1) С оглед по-голяма сигурност и намаляване на спама е желателно да се използват повече от един електронен адрес. Единият може да бъде само за служебна кореспонденция, а другият за лична. Препоръчва се електронният адрес за служебната кореспонденция да е на E-Mail сървъра на организацията, а другите са на някоя уеб базирана глобална поща.

2) Не трябва да се използват служебни електронни адреси за регистриране в различни форуми, социални мрежи и т.н. За тази цел е желателно да се направят няколко публични регистрации в общодостъпни уеб пощи и да се използват те, а не служебните. При това е желателно да се изберат E-mail доставчици, които прилагат много надеждни антиспам филтри.

3) Не бива да се отваря или още повече да се отговаря на електронно съобщение, което има характерните черти на спам. Това може да е реална примамка и открита възможност за получаване на още повече или по-нежелан спам, или фишингг атака.

4) Не трябва да се отварят прикачени файлове в съобщения, които са от неизвестен подател, или пък името записано в полето на подателите е непознато. Твърде вероятно е този файл да съдържа някакъв тип вируси. Дори и подателят да е известен, то прикрепеният файл може да е заблуда и поради това следва да се потърси потвърждение от подателя. В подобни случаи е нужно внимателно да се провери името и разширението за тип на прикачения файл.

5) Сигурната защита срещу нежелана кореспонденция е тя веднага да се изтрие без да се отваря. Това се отнася също и за съобщенията, съдържащи различни реклами. Те могат да бъдат използвани за прехвърляне на вируси от различно естество.

При подготовката на електронните съобщения много често се допускат грешки и неточности. Потребителите не винаги подхождат правилно и с необходимото внимание. Често изпратените съобщения са лишени от достатъчно идентифициращa информация, написани са формално и могат да бъдат дори подозрителни за получателите. За да не се допускат тези обстоятелства е необходимо да се избягват *често допускани грешки, по-съществените от които са:*

1) Недостатъчно добре и неясно се формулира темата на съобщението, която трябва да се запише в полето „Относно“ (subject): Дори в някои съобщения тя липсва или е съвсем формална. Според общоприетите правила темата следва да е кратка и да предоставя информация за какво се отнася писмото. Това може да се окаже истинската причина получателят да отвори и прочете това съобщение.

2) Много често съобщенията са твърде неясни, а понякога и пълни с правописни или други грешки. Желателно е преди съобщението да се изпрати, то да бъде ясно подготвено и изчистено от грешки. Най-добрият вариант за това е текстът на съобщенията да се подготвят в програма, която

проверява за правопис и след това да се прехвърли в полето за съобщение. Някои пощи правят проверки за правописен контрол, но не всички.

3) Друга често допускана неточност е липсата в края на съобщението на информация за изпращача. Препоръчва се във всяко електронно съобщение да се включва и информацията за подателя. Това може да се осъществява автоматично, чрез инструментите които предлагат програмите за подготовка на съобщенията. За тази цел собственика на електронната поща трябва само един път да въведе данните за себе си, като име, адрес, електронна поща, телефони за връзка и други, които той прецени. Те се въвеждат в специални полета и автоматично се пренасят в края на всяко подготвено съобщение.

4) Често допускана в практиката грешка е неправилно въведен или несъществуващ имейл адрес. По принцип програмите проверяват за действителен адрес, но понякога това може и да не се осъществи. В подобни случай или съобщението ще отиде до неправилния потребител, или пък въобще няма да се изпрати. Освен това не бива да се използва личната електронна поща за служебни цели и обратно. Това може да доведе до изтичане на информация, която има поверителен характер. Както вече стана дума, личната поща трябва да се предоставя в различни регистрационни процедури, като социални мрежи и други, но служебната в никакъв случай.

5) Като грешка в практиката може да се отчете и изпращането на големи прикачени файлове. Това, от една страна може да създаде сериозни проблеми на получателя, а от друга въобще да не прехвърли закачения файл. Ако за електронната поща на изпращача се знае какви файлове и с какъв обем могат да се прикачват и изпращат, то за получателя това няма как по принцип да се знае. Освен това няма яс-

нота какви са параметрите на връзката в Интернет, с която получателят на съобщението разполага.

Изпращане на големи по обем файлове не е проблем и за това съществуват други разнообразни стандартни процедури. Голяма част от тях се предлагат и като безплатни услуги за клиентите. При някои от електронните пощи тези услуги са интернирани към тях и са много лесно достъпни. Много често подобни услуги се наричат „облачни“, защото информацията на потребителя се съхранява в „облачни структури“. Това са информационни структури, които са достъпни с web адрес някъде в глобалното Интернет пространство.

Услугата „Google Drive“ е интегрирана с пощите създадени в Gmail. Това е „облачна услуга“, която позволява файловете за прикачване и прехвърляне да се съхраняват в специална папка с име Google Drive (Google Диск). Услугата се предоставя за абонати на Gmail и се инсталира от файла googledrivesync.exe, който следва да се изтегли от сайта. След инсталиране на програмата, на компютъра ще бъде създадена директория *Google Диск*. Директорията може да се използва за различни цели, включително и за прехвърляне на файлове. В този случай получателят на съобщението няма да има прикачен файл, а ще приеме само Интернет връзката към него. Свалянето на файла е елементарно и се свежда единствено до активиране на посочената връзка. За използване на Google Drive е необходимо услугата да се инсталира и да се направи достъп до нея. Това става с потребителското име и паролата за достъп до електронната поща в Gmail.

Услугата, която предлага Майкрософт се нарича „Sky Drive“ . Тя също е „облачна“ услуга и е интернирана в пощите на Hotmail. При нея се следи за обема на прикачените към съобщението файлове и ако се установи, че той надхвърля 25 MB се извежда съобщение за изпращача. В него се предлага прикачения файл да се препрати към създадения в SkyDrive акаунт. В случая в текста на съобщението ще има не прикачен файл, а препратка към него. Активирането на препратката ще прехвърли файла върху компютъра на получателя.

Налице са и много други сайтове, които не са свързани с конкретни електронни пощи и предлагат услугата прехвърляне на файл. При голяма част от тях не са нужни регистрации и процедурата по закачане на файловете е много елементарна. Особеното тук, че голямата част от тях съхраняват файловете и ги предоставят за достъп само за определено време. След изтичането на това време файловете се изтриват автоматично. Има и услуги за прехвърляне на файлове, които позволяват да се поставят пароли за достъп до тях.

Доста популярен сайт, които предлагат такива услуги е например File dropper (http://www.filedropper.com/). Той позволява качване на файлове до 5 GB и ги съхранява за срок до 30 дни от момента на последното им сваляне. Ако се прави периодичен достъп до тях, за срокове по-малки от 30 дни, то фаловете няма да бъдат изтрити. Използването на услугата на този сайт е много елементарна и се свежда до качване (Upload) на желания файла в сайта. Той ще предложи линк към него, който следа да се запише и използва при нужда файла да се сваля от потребителя. Ако файловете вече са в сайта, то при подготвяне на електронни съобщения, вместо прикачване на файл, може да се използва и посочва на получателя линка към този файл. За вмъкване на линкове електронните пощи предлагат специален инструмент. Той най-често се казва „*Вмъкни линк*“ (*Insert Link*) и е налице във всяка електронна поща.

Средство за изпращане на големи файлове е и популярният български сайт DOX.bg. Той позволява изпращане и съхранение на информация с обем до 3 GB. Сайтът е ориентиран основно към пощи създадени, чрез abv.bg, но може да се използва и от всички потребители на Интернет услуги. Работата с него е аналогична на тази, която беше описана по-горе, но обемът от представено пространство за съхранение на файловете е ограничен до 3GB. Освен това всеки отделен файл не може да има големина по-голяма от 1 GB, което си е ограничение за практиката. Свалянето на файловете от сайта се извършва от клиента и не е фиксирано по време. Потребителският интерфейс за работата със сайта е лесен и се разучава за кратко време.

Налице са и много други сайтове, които предлагат услугата за прехвърляне на големи файлове. Така например услугата WeTransfer (https://www.wetransfer.com/) позволява да се изпращат файлове до 2 GB. Те обаче са достъпни за изтегляне само за две седмици, а това си е сериозно ограничение. За разлика от File Dropper, в тази услуга не се налага да се копира връзка към файла в имейл съобщението. Там трябва да се да се посочи имейл адреса на получателя. Услугата предлагана от Ddropbox (https://www.dropbox.com/) е подобна на описаните, само че там позволения обем на файловете е до 2 GB. Възможно е и за по-големи обеми, но тогава трябва да се търси комерсиалната версия на програмата, а не безплатната.

При работата с електронни пощи могат да се посочат и редица други подобни сайтове или пък отделни програми, чрез които да се осъществява обмен на големи файлове. При всички от тях файловете не се прикрепват към съобщението, а в него се внася информация за наличието на такъв файл и как да се свали той.

Обмена на файлове в Интернет е често срещаната дейност, която потребителите непрекъснато ползват. В този случай използването на услугите на електронните пощи става доста неудобно и нецелесъобразно. Неудобно и зависимо от много фактори е и прехвърлянето на файлове чрез безплатните „облачни структури“. Това налага да се прилагат други по-ефективни и по-надеждни методи, които Интернет предлага. Една от тях, масово използвана от потребителите, е дистанционният достъп и управлението на компютри, които са свързани в локални мрежи и/или в Интернет.