

**Коммерциялық емес
акционерлік
қоғам**



**АЛМАТЫ
ЭНЕРГЕТИКА
ЖӘНЕ БАЙЛАНЫС
УНИВЕРСИТЕТІ**

*Ақпараттық
жүйелер
кафедрасы*

WEB-ТЕХНОЛОГИЯЛАР

5B070300 – Ақпараттық жүйелер, 5B060200 – Информатика
мамандықтарының студенттеріне арналған дәрістер жинағы

Алматы 2016

ҚҰРАСТЫРУШЫЛАР: Ш.И.Иманғалиев, Н.А.Дауренбаева. Web-технологиялар. 5В070300 – Ақпараттық жүйелер, 5В060200 – Информатика мамандықтарының студенттеріне арналған дәрістер жинағы. – Алматы: АЭЖБУ, 2016. – 47 б.

Дәрістер жинағы «Web-технологиялар» бағдарламалық курсына сәйкес 5В070300 - Ақпараттық жүйелер, 5В060200 - Информатика мамандықтарының студенттеріне арналған. Дәрістер жинағында web-технологиялар негіздері, Интернет желісіне қатынас жасау технологиялары, Интернеттегі web-серверлер, статистикалық және динамикалық web-сайттар, Интернеттегі ақпарат қауіпсіздігі, іздеу машиналары, электронды цифрлық қолтаңба, Интернеттегі қолданушы идентификациясы, web-технологияның даму болашағы қарастырылған.

Библиография - 7.

Пікір беруші: к.т.н., доцент Матаев У.М.

«Алматы энергетика және байланыс университеті» коммерциялық емес акционерлік қоғамының 2016 жылғы жоспары бойынша басылады.

© «Алматы энергетика және байланыс университеті» КЕАҚ, 2016 ж.

АННОТАЦИЯ

на конспект лекции по дисциплине «Web-технологии»

Целью курса «Web-технологии» является обучение методам проектирования приложений для использования в среде Интернет, а также освоение технологий, принципов организации и функционирования Интернет. В рамках данного курса рассматриваются следующие:

- структура и принципы Web (базовые понятия, архитектура, стандарты и протоколы);
- технологии сети Web (языки разметки и программирования web-страниц, инструменты разработки и управления web-контента и приложений для Web, средства интеграции web-контента и приложений в Web);
- взаимодействие компьютеров через Интернет. Технология доступа к сети Интернет;
- статистические и динамические WEB-сайты. Технология CGI;
- защита информации в Интернет. Криптография и Интернет;
- идентификация пользователей в Интернет. Механизм Cookies;
- технологии создания клиентских приложений Интернет;
- перспективы развития WEB-технологий и образовательный процесс.

Мазмұны

1 Дәріс №1. Web - технологиялар негіздері. Web стандарттары және олардың дамуы.....	4
2 Дәріс №2. Интернет коммуникациясының моделі. Коммуникацияның Pull- және Push-моделі. Интернет сервисінің коммуникациялық сипаттамалары.....	9
3 Дәріс №3. Қолданушының Интернетке кіруі. «Соңғы миля». Коммутация каналының желісі. Модем.....	13
4 Дәріс №4. Интернет жүйесіне қатынасу технологиялары. DSL, ISDN технологиялары.....	17
5 Дәріс №5. Интернеттегі web серверлер. Web – сервер жұмысының механизмі. Статистикалық және динамикалық беттер. CGI технологиясы. Скриптер.....	21
6 Дәріс №6. Web-ресурстарды алу технологиясы. Web-парақтарды кәштау. Прокси-сервер механизмінің жұмысы.....	24
7 Дәріс №7. Интернеттің іздеу технологиялары.....	27
8 Дәріс №8. Интернет сервистері. Электрондық пошта. E-mail сервисінің жұмыс істеу механизмі. E-mail-дің екі протоколы. Электрондық поштаның адресі.....	32
9 Дәріс №9. Интернет сервисі. Файлдармен алмасу. FTP сервисінің жұмыс механизмі. FTP – клиенттер.....	36
10 Дәріс №10. Интернеттегі мәліметтерді қорғау. Цифрлық қолтаңба. Криптография және Интернет. Симметриялық және асимметриялық кілттер. Цифрлық қолтаңбаның механизмі. Қауіпсіздік проблемалары.....	39
11 Дәріс №11. Интернетте пайдаланушыларды идентификациялау. Cookies механизмі. Cookies-ті қолдану. Cookies негізіндегі технологиялардың кемшіліктері.....	44
Әдебиеттер тізімі.....	47

1 Дәріс №1. Web - технологиялар негіздері. Web стандарттары және олардың дамуы

Дәрістің мақсаты: байланысқан желілер, клиент-сервер түсініктерімен таныстыру.

Дәрістің мазмұны: «Желі» терминінің түсінігі. Клиент-сервер архитектурасы. Провайдерлер және олардың желілері. Компьютерлер-серверлер және компьютерлер-клиенттер. Қосымша-серверлер және қосымша-клиенттер. Провайдерлер желілерінің иерархиясы.

Қазіргі кезде Internet те телефон, факс, сияқты адам өмірінің ажырамас бөлігі болып табылады. Адамдардың барлығы қандай да бір ақпарат алу, бір-бірімен сөйлесу мақсатында Internet деп аталынатын дүниежүзілік өрмекте саяхат жасайды.

Интернет дегеніміз глобальді желі. Интернет физикалық мағынасында бір-бірімен байланыс линиялары арқылы байланысқан бірнеше миллиондаған компьютерлер деп қарастыруға болады. Бірақ Интернетті физикалық мағынада емес, оны ақпараттық кеңістік деп қарастырған дұрыс.

Интернетті ішінде мәліметтердің үздіксіз циркуляциясы жүретін кеңістік ретінде қарастыруға болады. Интернеттің теле және радиоэфирден айырмашылығы – эфирде ешқандай ақпарат сақталынбайды, ал Интернетте ол желінің түйіндерінде болатын компьютерлер арасында орын ауыстырады да, қандай да бір уақыт аралығында қатты дискіде сақталады.

Екі немесе одан да көп компьютерлер арасындағы физикалық байланысу компьютерлік желі деп аталынады. Жалпы компьютерлік желілерді құру үшін арнайы аппараттық қамсыздану және арнайы бағдарламалық қамсыздану қажет.

Компьютерлік желілер аппаратты ресурстардан басқа қосымша программалық ресурстарды да пайдалануға мүмкіндік береді. Компьютерлік желілер локальді және глобальді болып бөлінеді.

Интернет – глобальді желі. Қазіргі кезде әлемде 200-ден астам глобальді желі бар. Барлық әлемдегі глобальді есептеуіш желілер өзара Интернет көмегімен байланысқан.

ҒЕЖ-де жұмыс істеу үшін сәйкес аппаратты және программалық қамсыздану болу керек. Барлық қамсыздану 2 топқа бөлінеді:

1) Бағдарлама-серверлер - қолданушының компьютеріне қызмет көрсететін желі түйінінде орналасатын бағдарламалық қамсыздану.

2) Бағдарлама-клиенттер – қолданушының компьютерінде орналасады және сервердің қызметін пайдаланатын бағдарламалық қамсыздану.

Заманауи интернет технология бір орында тұрмайды. Қазіргі кезде адамның күнделікті өмірін интернеттің көмегінсіз елестету мүмкін емес. Интернет ол әлемдегі ең үлкен желі. Оның бірегей басқару орталығы болмайды, бірақ ол белгілі бір ереже бойынша жұмыс жасайды және өзінің қолданушыларына қызметтер жиынтығының бірегейлігін ұсынады. Интернетті «желілердің желісі» ретінде қарастыруға болады, олардың

әрқайсысы бір-біріне тәуелсіз операторлармен басқарылады – Интернет қызметінің провайдерлері (ISP, Internet Service Provider).

1. Өзара әсерлесетін және бір-бірімен байланысқан компьютерлер тобы өрмекті құрайды. Интернет – бүкіл әлем бойынша таратылған мыңдаған кіші желілерден тұратын компьютердің үлкен өрмегі.

Интернеттегі компьютерлер бір ортақ тілде сөйлеседі, ал бұл тіл протоколдарда бекітілген.

Протокол деген желідегі компьютерлердің өзара әрекеттесу механизмін анықтайтын жалпыға бірдей ережелер жиынтығы. Интернеттегі мәліметтермен алмасуға арналған стандартты протоколдар: TCP және IP. Осы екі протоколдың комбинациясы TCP/IP түрінде болады.

2. Интернетке қатысты қолданылатын терминдер:

1) Айна - алыста орналастырылған атақты сервердің көшірмесі болатын сервер.

2) Прокси-сервер - желідегі жүктемені төмендететін және желідегі іс-әрекетті тездететін компьютер.

3) Шлюз - әртүрлі протоколдармен жұмыс жасайтын әр текті екі желіні біріктіретін бағдарламалық-аппараттық құрал.

4) Брандмауэр – қорғауға алынған желіге санкциясыз енуді тоқтатын аппараттық құрал.

5) Маршрутизатор – бірнеше каналдармен жұмыс істейтін құрылғы.

6) Маршрутизациялау – ақпараттың жіберілу жолын таңдау процедурасы.

3. Интернет көптеген әртүрлі ұйымдардың компьютерлерін біріктіретін болса, Интранет бір ғана ұйымның ішіндегі компьютерлерді біріктіреді. Интранеттегі ақпарат тек қана сол ұйымның адамдары пайдалана алады. Интранет желілері электронды пошта секілді бизнес үшін өте тиімді коммуникациялық құрал болып табылады.

Қазіргі таңдағы Интернет желісі, өзінің қарқынды дамып келе жатқаны үшін ARPANET біріктірілген желісіне қарыздар. Бұл желі коммутация пакеттері технологиясының қарапайым эксперименті ретінде басталған.

Интернет өте күрделі желі болып табылғандықтан, сәйкесінше, желі құрылғылары арасында қарым-қатынасты ұйымдастыру тапсырмалары да күрделі болып келеді. Мұндай күрделі тапсырманы шешу үшін декомпозиция қолданылады. Бұл дегеніміз күрделі тапсырмаларды бірнеше қарапайым тапсырма-модельдерге жіктеу.

Интернет сөзі Interconnected networks (байланысқан желілер) терминінен шыққан, яғни техникалық көзқараспен – бұл кіші және ірі желілер бірлестіктері. Кең мағынасында – бұл, бір-бірімен мәліметтер алмасатын жер жүзіндегі миллиондаған компьютерлер арасында бөлінген ақпараттық кеңістік. Көбіне Интернет сөзімен Желінің ақпараттық құрамын түсінеді. Интернет – бұл өзіне уникальды жетістіктерді толығымен жинаған

технология. Интернет сонымен қатар, ең күшті және тәуелсіз ақпарат қоры, байланыстың сенімді және оперативті тәсілі, жер жүзіндегі миллиондаған адамдардың шығармашылық түрде өзін-өзі көрсету және ақпараттық технологияларды дамыту негізі болып табылады.

Интернеттің басты тапсырмасы бұл – әр тәуліктік, жоғары сенімді байланыс. Интернетке қосылған кез келген екі компьютер (немесе басқа құрылғылар) бір-бірімен кез келген уақытта хабарласа алады. Ары қарай «Желі» сөзін қолданғанда Интернет сөзіне синоним ретінде Желімен интернет арқылы екі компьютерді байланыстыру мүмкіндігін және олардың өзара байланысын қамтамасыз етуді түсінеміз. Интернетке қосылған әрбір компьютер – бұл Желінің бір бөлігі.

Компьютерлер-серверлер және компьютерлер-клиенттер.

Интернетке қосылған барлық компьютерлерді екі типке бөледі, олар :серверлер және клиенттер. Бір компьютерде серверді де және клиентті де орнату мағынасында бөлу онша қатаң жүргізілмейді. Жергілікті компьютерде Web-сервер орнатылуы мүмкін және осыған қарамастан, дәл осы компьютерде браузермен және почталық клиентпен де жұмыс жасауға болады.

Басқа компьютерлерге анықталған сервис ұсынатын компьютерлерді *серверлер* (ағыл., *to serve* – қызмет көрсету) деп атайды, ал осы сервисті қолданатындар - *клиенттер*.

Көп жағдайларда үйдегі клиенттік компьютерлерде әр уақытта Интернетке кіруге мүмкіндігі болмайды, сондықтан Желіге тек керек уақытта ғана қосылады. Керісінше, компьютер-серверлер мәліметтерді берудің жоғары жылдамдықты арналары арқылы Интернетпен байланысқан, сондықтан оларға сұраныс арқылы хабарласуға болады.

Қосымша-серверлер және қосымша-клиенттер.

Компьютерлерді серверлер мен клиенттер деп атағаннан гөрі, оларды бағдарламалық қамсыздандыру деңгейіндегі клиенттер немесе серверлер деп атаған жөн. Бір бағдарлама клиент есебінде, ал екіншісі сервер есебінде іске қосылатын қосымшалардың өзара байланысы *клиент-сервер архитектурасы* деп аталады.

Сервердің басты тапсырмасы – сервиске қайсыбір клиент сұраныс жібермейінше әр кезде жұмыс жасап және күту жағдайында болу болып табылады.

Серверде сұраныстардың көптігінен оның жұмысы баяулап және белгілі бір сұраныстарға қызмет көрсетуді тежейді. Серверге сұраныс белгілі бір протокол шегінде болады – бұл Желіде компьютерлер арасында байланысты қамтамасыз ететін стандарттар жиыны. Серверлік бағдарламалар клиенттік бағдарламаларға қызмет көрсету үшін компьютердің аппаратты ресурстарын қолданады. Клиент-бағдарлама сұраныс құрып, оны желі арқылы белгілі бір адреске жібереді және алдын ала белгіленген протокол арқылы сервер-бағдарламамен өзара байланысады. Сол бір компьютерде бірнеше серверлік бағдарламалар

орналаса алады. Клиенттік қосымша серверлік қосымша орналасқан компьютерде де, сонымен қатар, серверден керегінше жойылған компьютерде де орналаса алады, бірақ олар Желімен байланысса, бұл айырмашылық тек уақыт бойынша жауаптың кідіруіне сәйкестеледі.

Әрбір сервер-бағдарламаның типі үшін өзіндік клиент-бағдарламасы бар. Осылай, Web-клиент Web-серверге, почталық клиент – почталық серверге хабар береді және т.б. Серверлік бағдарлама әрқашан сұранысты орындауға дайын болу керек және сондықтан да сервер-бағдарлама жұмыс жасайтын компьютерлерге сенімділікке және өнімділігіне байланысты жоғары шарттар қойылады. Клиенттік компьютердің жұмысының тұрақтылығы бір адамның жұмысына әсер ететіндіктен, олардың жұмысына сенімділігіне байланысты аз талаптар қойылады, ал аппаратты сервердің жұмысының сенімділігіне байланысты көптеген клиенттердің жұмысының жүргізілуі тәуелді болады. Жоғарыда көрсетілген тәсіл (клиент-серверлік архитектура) дербес компьютердің қолданушысына өзінің жұмыс үстелінен Интернетке қосылған миллиондаған серверлердің ресурстарына қол жеткізуге мүмкіндік береді.

Провайдерлер және олардың желілері.

Интернетке қарап, біз интернет-провайдерлердің қызметтерін пайдаланамыз және ISP(Internet Service Provider – Интернет қызметін жеткізуші). Көбіне ISP – бұл өзіндік желісі бар арнайы ұйым (магистральды деп аталады), оған клиенттердің көптеген саны қосылады. Провайдердің желісі ғаламның кез келген нүктесімен байланысуды қамтамасыз ететін жер жүзінің басқа да желілерімен байланысуы мүмкін. Қалыпты жағдайда ISP-провайдерлер – бұл белгілі бір аймақтарда өзіндік орналасу нүктесі (POP - Point of Presence) бар ірі компаниялар, бұл нүктелерде клиенттерінің Интернетке қосылуын қамтамасыз етуге арналған провайдердің аппаратты қамсыздығы. Ірі провайдердің әртүрлі қалаларда өзінің орналасу нүктесі мен мыңдаған клиенттері болады. Бірнеше қалаларда орналасу нүктелері бар провайдерлермен қатар, бір қалада орналасу нүктесі бар провайдерлерді де атап көрсетуге болады. Телефон линиясы арқылы ISP мен байланысуды ұйымдастыру: ДК қолданушысы драйверге хабарласады және модем жинақтарының ішіндегі провайдер модемдерінің бірімен байланыс орнатады (модемді пул деп атауға болады). Қолданушы өзінің ISP не қосылғаннан кейін, ол оның желісінің бір бөлігі болып табылады. Провайдер өзінің серверінде клиенттерге әртүрлі қызмет көрсете алады: электрондық почта (e-mail), желілер жаңалықтары (Usenet) және т. б. Провайдердің магистральды желісін көбіне тіректі желі немесе бэкбоун деп атайды (ағыл. Backbone-қырат). Провайдер желілері көптеген клиенттерге қызмет көрсететіндіктен, оның жоғары жылдамдықты желісі болуы және жоғары трафикті қамтамасыз етуі керек (желі бойымен берілетін мәліметтер көлемі). Өзінің барлық орналасу нүктелерін біріктіру үшін, провайдер ірі коммуникациялық компаниялардан жоғары жылдамдықты арналарды жалға ала алады, сонымен қатар, өзінің арналарын тарта алады. Ірі

коммуникациялық компаниялардың өздерінің жоғары жылдамдықты каналдары бар.

Провайдерлердің желілерін біріктіру.

Кейбір провайдерлердің клиенттері, мысалы, ISP-A бір бірімен өздерінің жеке желілері арқылы өзара байланысады, ал басқа ISP-B компаниясының клиенттері өздерінің, бірақ егер ISP-A және ISP-B желілерінің арасында байланыс болмаса, онда А компаниясының клиенттері және В компаниясының клиенттері бір бірімен байланыса алмайды. Өздерінің клиенттерін бір желіде біріктіру мақсатында А және В әр қалада желілік кіруді (NAP - Network Access Points) қамтамасыз ететін нүктелер арқылы өз араларында тікелей байланысты орнатады. Осылайша, басқа провайдерлердің магистральды желілеріне қосылуы құрылады, нәтижесінде жоғары деңгейлі көптеген желілердің бірігуі болады.

Интернетте жүздеген ірі интернет-провайдерлер орналасады және олардың магистральды желілері NAP арқылы әртүрлі қалаларда жасалады, және мәліметтердің үлкен ағыны NAP-түйіннің әртүрлі желілері арқылы таралады.

Үлкен және кіші желілердің бірігуі (Интернетті құрайтын) негізінде шартты келісімдер жатады. Әрбір клиенттің белгілі бір ISP пен өзінің компьютерін немесе жергілікті желісін провайдер желісіне қосу туралы келісім шарты бар. Кейбір ISP-A провайдерлердің клиенттері ISP-A желісіне қосылу туралы келісім құрайды, өз кезегінде ISP-A ISP-B мен желілерін біріктіру туралы келіседі және солай жалғаса береді.

Провайдерлер желілерінің иерархиясы.

Әртүрлі елдерде халықаралық, ұлттық және аймақтық болып бөлінетін жүздеген провайдерлер бар.

Аймақтық провайдерлердің желілері (екіншілік) ұлттық провайдерлердің желілерімен (біріншілік) жоғары жылдамдықты каналдар арқылы байланысады. Мысалы, АҚШ-та T1 стандартты мәліметтерді беру жылдамдығы 1,544 Мбит/с арна немесе жылдамдығы 44,74 Мбит/с жететін T3 арнасы.

Осыдан он жылдай уақыт бұрын Microsoft корпорациясы веб-стандарттарды құруды қолға алды. Бұл веб-стандарттар қорыта келе, барлық веб-бағдарламалау бойынша берілетін технологияларды бір бүтін етіп жинақтауға және көшірілетін веб-платформаны құруға бағытталған.

Бақылау сұрақтары:

- 1) Клиент-серверлік архитектураны құрайтын негізгі желілер қандай?
- 2) Желіні бағдарламалық қамсыздандыру қандай принциппен жүргізіледі?
- 3) Провайдердің магистральды желі термині нені білдіреді?
- 4) Провайдерлер желілерінің бірігуі қалай орындалады?
- 5) Интернетті түзетін желілер иерархиясы қалай аталады?

2 Дәріс №2. Интернет коммуникациясының моделі. Коммуникацияның Pull- және Push-моделі. Интернет сервисінің коммуникациялық сипаттамалары

Дәрістің мақсаты: интернет коммутациясының модельдерін, интернет сервисінің коммуникациялық сипаттамаларын таныстыру.

Дәрістің мазмұны: интернет коммуникациясының Pull- және Push-модельдері. Интерактивтілік. Гипермәтін. Мультимедиа. Болау эффектісі. Желілік навигация. Internet сервисінің коммуникативті сипаттамасы.

Интернет коммуникациялық сипаттамаларын қарастырайық. Дәстүрлі коммуникациялық модель негізінде «бірге бір» ережесі жүреді. Коммуникациялық құрылымға байланысты ақпарат статикалық (мәтін, графика) және/немесе динамикалық (аудио, бейне, анимация) күйінде көрсетіледі.

Бұл модельден ерекше Интернет негізінде екі басқа принциптер жатыр. Біріншіден, Байланысқа өз үлесін қосатын Интернетке коммуникация кезінде оның арнасы арқылы өтеді. Бұл модель бастапқы байланыс жіберуші мен қабылдаушы арасында емес, негізінде қолданушы мен коммуникациялық ортадағы бір кеңістік арасында болатынын көрсетеді, сонымен байланыстың екі қатысушысы да жіберуші де, қабылдаушы да болып табылады.

Интернет өзімен әрбір желі абоненті басқа абоненттерге немесе топтармен топ атымен немесе өз атымен хабарласа алтын «көпке көп» көп бағыттылы коммуникациялық модельді көрсетеді. Бұл модельде коммуникация құралы болып таратылған компьютерлік желі айтылады, ал ақпарат гипермедиялық түрде көрсетілуі мүмкін. Бұл модель интерактивті байланыс Интернеттің басқа қолданушыларымен қатар ортаның өзімен де бола алатынын, тіпті соңғы байланыстың соңғы түрі басымдылық көрсететінін білдіреді. Осындай байланыстың бар болуынан ақпарат жіберуші құралы кейде оның қолданушысы да бола алады. Бұндай модельде ақпарат және мазмұн жіберушіден қабылдаушыға беріліп қана қоймай, ортаның өзі де оның қатысушыларымен де құрылады.

Интернет ортасының моделі ашық көрсетілген кері байланыстарды көрсеткенде, жалпы коммуникацияның дәстүрлі әдістері үшін коммуникациялық модельде кері байланыс контуры болмайды. Тұтынушымен кері байланысты жүзеге асыруға мысал ретінде электронды почтаны, қолданушылар тіркеу туралы мәліметтер, «cookie» файлдары, Web-серверлерде жазылу немесе тіркелу. Кері байланыстың болуы өзара байланыстың коммуникациялық әдістерін қолдану тиімділігін және ішкі және сыртқы ортада болатын оқиғаны қалыпты қабылдауды жоғарылатады.

Интернет коммуникациясының Pull- және Push-модельдері.

Жалпыға бірдей қызмет көрсетудің дәстүрлі әдістері тұтынушыларға ақпаратты жеткізуші push-модельді жүзеге асырады, бұнда тұтынушылар пассивті роль атқарады және ақпараттың каналдарын таңдаудың шектеулі мүмкіндіктерінің болуы.

Ақпаратты жеткізудің дәстүрлі push-моделіне қарсы Интернет негізінде, ақпаратты сұраныс бойынша жеткізетін (demand pull) pull-моделі жатыр. Бұл Интернет ортасының ерекшелігі ақпаратты іздеуде бақылаумен негізделген және іздеу механизмін қолдануда навигация бейнесі немесе басқа да URL (uniform resource locator) бастауларына байланысты тұтынушылардың тікелей қатысуымен байланысты. Интернетте сонымен қатар push-моделін іске асыру мүмкіндігі бар. Интернет бұл модельмен push-технологиясы арқылы жүре алады, соған байланысты қолданушыларға Интернетте ақпаратты іздеп жатудың қажеті жоқ, ол тек керекті тақырып бойынша қажетті каналға жазылса болғаны, кейін ақпарат канал жазылушыларының компьютерлеріне автоматты түрде жеткізіліп тұрады.

Интернет ортасының технологиялары push- және pull-модельдерінің тығыз байланысы бағытында дамиды. Интернеттің жоғары функционалдылығына байланысты керекті ақпаратты немесе басқа да қорларды табу мақсатында қолданушының навигация мүмкіндіктері әрқашан да болады. Басқа жағынан, қолданушылардың әрқашан ақпаратты жеткізушіні және қабылданатын push-каналдар тематикасын таңдауға мүмкіндіктері бар.

Интерактивтілік.

Internet ортасының басты сипаттамасы оның интерактивтілігі болып табылады. Интерактивтілік – бұл коммуникациялық хабарламалардың бір біріне қатысты орналасуын білдіретін, коммуникация процесінің жүзеге асуын көрсететін сипаттама. Интерактивтік өзара байланыс үшін ақпараттың немесе хабарламаның келуіне жауапты іс-әрекеттің болуы тән, сонымен қатар жауап алдындағы хабарламаның контекстінде болуы қажет.

Жоғарыда айтылғандай, Интернет ортасы үшін интерактивтілікті қолданушыға «жауап қайтару» мүмкіншілігі есебінде түсінуге болады. Осылайша, Интерактивтілік компьютердің қолданушының қимылын бағалап және осы бағаға байланысты жауап бере алатын мүмкіндігі бар, диалогқа қатысушы есебінде функциялық көрінісін кеңейтеді және толықтырады. Компьютерлік гиперортаны қолдану арқылы өзара байланысу процесінде клиентпен хабарласу қатынасты орнатудың ең бастапқы кезеңінде сол компьютерлік гиперортамен, клиенттің алдыңғы іс-әрекетке қалай қарағандығына байланысты жасалуы мүмкін. Internet негізінде жатқан құрамдық модельді қайта қарау барысында, Internet ортасындағы интерактивтілік енді орта арқылы жеке қатынас деңгейінде жүзеге аспай, нақты ортаның өзімен өзара байланысу деңгейінде жасалатынын көруге болады.

Өзара байланыстың интерактивті сипаты коммуникация мүшелерінің өзара байланысу әсерін жоғарылатуға мүмкіндік береді. Бұл, мысалы

тәжірибе жүзінде, келісім немесе сатып алу үшін қажетті ақпаратты алу үшін кететін уақытты қысқартуға керек. Сонымен қатар, ортаның интерактивті сипаты жеке клиенттің ерешеліктеріне қатысты байланыстың қалыптасу мүмкіндігін ұсынады.

Гипермәтін.

Internet ортасының гипермәтіндік табиғатының ерекшелігі аз емес. Гипермәтінге негізделген дүние жүзіндегі ең алғашқы жүйені бірнеше жылдан астам уақыт бұрын ЭЕМ-нің алғаш құрушыларының бірі (Ванневар Буш) ұсынған. Бұл жүйе Метех деп аталады, ол қолданушының жеке кітаптарын, жазбалар мен коммуникацияларын сақтайтын құрылғы, оған жүктелу тез және оңай. 1967 жылы Нельсон (Nelson) гипертексті жүйелер көрсеткіштері мен ассоциация ретінде бейнелеп, адам ойындағы жеке мәліметтер бөліктерін ұйымдастыру және байланыстыру мүмкіндіктеріне теңеді. 1993 жылы Бомман (Bomman) гипертекстке мынандай анықтама берді: «Гипертекст концепцияның ретсіз жазба мәліметтерін құрайды, осыған орай қолданушы мәліметтер бөліктерін бір-бірімен көрсеткіштер мен байланыстар көмегімен байланыстырады. Гипертекстік жүйеде мәлімет түйін және байланыс түрінде беріледі».

Гипертекст ұйымдастыру құралының бөліктерге бөлінген сызықты емес желілер формасымен сипатталады. Мұнда әр бөлік (фрагмент) келесі бөлікке белгілі бір байланыс типі арқылы көшеді.

Гипертекст мәліметтерді ғана емес, сонымен бірге қолайлы іздеу қондырғысын құрайды. Сонымен, гипертекстік көрініс мәліметтері қарапайым әдіске қарағанда, мәліметтерді қорытады.

Мультимедиа.

Мультимедияның пайда болуына байланысты динамикалық (аудио, видео, анимация) және статикалық (текст, графикалар, суреттер) құрамы бар компьютерлік интеграция мүмкіндігі туды. Түйіндер мен байланыстар комбинациясы гипертекстік жүйе мультимедиясында жаңа ортаны құруға мүмкіндік берді.

Гипермедиа – бұл мәліметтер көрінісі және оған кіру әдісі. Оның концепциясы граф түрінде берілген мәліметтер кеңістігінің моделінде орналасады, түйіндерінде мәліметтер, ал семантикалық байланыс граф доғасында қамтылады. Ақиқатты гипермедиа жүйесіндегі сақталатын мәлімет осы заманғы компьютер шығара алатын барлық мүмкін формалармен көрсетіледі. Сонымен қатар, гипермедиа өзінде радио (аудио), теледидар (динамикалық бейне), пресса (текст, суреттер, фотосуреттер) және компьютер (видеотерминал) компьютерлік гиперортада құрамында жататын гипертекстік байланыстарды орнатады.

Болу эффектісі.

Интернеттің коммуникациялық моделінің басты мәселесі «болу эффектісі» болып табылады, қоршаған ортамен клиенттің араласу процесі: жағдай, бөлме, компьютерлік жұмыс орын және т.б., компьютерлік гиперәдіспен құралатын орта құрамына кіреді. Дәреже қатынасы мен

клиентке әсер ету «болу эффектінің» дәрежесін анықтайды. Айта кеткен жөн, «болу эффектісі» өзінің табиғатына сай, интерактивтік араласу мен компьютерлік гиперортамен тығыз байланысты.

Желілік навигация.

Желілік навигация компьютерлік гиперортада өзіндік қозғалыс процесі болып табылады. Сызықты емес іздеуді және мәліметтерді талап ету құрамындағы әдісті клиентке еркін түрде береді.

Internet сервисінің коммуникативті сипаттамасы.

Интернет комплексті сервис болғандықтан, оның жеке сипаттамаларын таңдап және қолдану кезінде көрсету керек. Кестеде коммуникация түріндегі Internet коммуникациялық сервис анализінің нәтижесі, коммуникация моделінің құрамында жатқан, көрсетілген мәліметтер түріне, симметриялық кері байланыс және интерактивті қарым-қатынасы көрсетілген.

2.1 кесте - Internet сервисінің коммуникативті сипаттамасы

Сервис	Аралық қарым-қатынас	Машиналық қарым-қатынас	Коммуникация Моделі	Мәліметтер түрінің көрінісі	Кері байланыс симметриясы	Интерактивті қарым-қатынас мүмкіндігі
Электрондық пошта	Иә	Иә	Бірге-бір Бірден – көпке	Мәтін, графика, дыбыс	Иә	Жоқ
Жіберу тізбегі	Иә	Иә	Көпке-көп	Мәтін	Иә	Жоқ
Конференциялар	Иә	Иә	Көпке-көп	Мәтін	Иә	Жоқ
Сөйлесу бөлімдері	Иә	Иә	Көпке-көп	Мәтін	Иә	Иә
WWW	Иә	Иә	Көпке-көп	Мәтін, графика, дыбыс, видео	Жоқ	Иә
Дауыс байланысын ың программалары	Иә	Иә	Бірге-бір	Дыбыс	Иә	Иә
Аудио- және видео-конференциялары	Иә	Жоқ	Көпке-көп	Дыбыс, бейне	Иә	Иә

Көрсетілген мәліметтер Интернет ортасының қолдану әдістерінің коммуникациялық кең диапазонды түрлері көрсетілген. Нақты есептерді шығару кезінде әрбір Интернет сервисінің жеке анализдері қажет.

Бақылау сұрақтары:

- 1) Қандай коммуникативті модельдер Интернетте шығарылады?
- 2) Гипертекст ұғымы нені білдіреді?
- 3) Internet ортасындағы интерактивтік ұғымы нені білдіреді?
- 4) Pull- және Push-моделдерінің Internet коммуникациясының ерекшеліктері қандай?
- 5) «Болу эффе́ктивтісі» термині Internet ортасында нені білдіреді?

3 Дәріс №3. Қолданушының Интернетке кіруі. «Соңғы миля». Коммутация каналының желісі. Модем

Дәрістің мақсаты: қолданушының интернетті пайдалану кезіндегі «соңғы миля», «коммутация каналының желісі» және «модем» түсініктерімен, интернетке кірудің түрлі нұсқаларымен таныстыру.

Дәрістің мазмұны: «Соңғы миля» технологиясы. Желінің коммутациялы каналдары. Модем функциясы. ASCII-кодировкасы.

Бірнеше компьютерлер арасында жобалау және есептерді шығаруды жеңілдету үшін ол жүйені бірнеше бір-бірімен байланысқан топтарға бөлінеді. Жүйе арқылы алмасу жүріп жатқанда екі торап келесі ережелерді сақтауы тиіс:

- электрлік сигналдардың түрін және деңгейлерін келістіру;
- берілістердің ұзындығын анықтау әдістері;
- бақылау әдістері.

Келісімдер мәліметтерді интерпретациясын анықтайтын, биттарды беру ең кіші деңгейден үлкен деңгейлерге дейін барлық деңгейлерге бірдей болу керек.

Бір деңгейдегі берілістердің форматын және тізбегін анықтайтын ондай формалданған ережелерді протоколдар деп атайды.

Иерархиялық жүзеге асырылған протоколдардың жиынтығын коммуникациялық протоколдардың стеки деп атайды.

Желілік деңгей біріншіден келесі есептерді шығару үшін құралдармен қамтамасыз ету керек:

- еркін топологиясы бар желілерге пакеттерді жеткізу;
- желіні сенімді локалды трафиктың арқасында құрылымдау;
- әртүрлі протоколдардың каналдық деңгейледің келісуі.

Желідегі трафик кездейсоқ ретімен орналасады, бірақ онда кейбір заңдылықтар көрсетіледі. Кейбір жалпы есеппен жұмыс істейтін қолданушылар (мысалы, бір бөлімнің қызметкерлері) көбінесе бір-біріне немесе жалпы серверге сұраумен қатынасады. Сол кезде олардың басқа бөлімдердің компьютерлерінің ресурстарымен қолдануы қажет болады. Сондықтан жүйенің құрылымы мәліметтердің ағынының құрылымына сәйкес келу керек. Жүйедегі трафигіне байланысты компьютерлер бірнеше

бөлімдерге (сегменттерге) бөлінуі мүмкін. Егер бір-бірімен қатынасатын компьютерлердің сұраулары мен жауаптары осы топтың компьютерлеріне арналса, онда олар бір бөлімге жинақталады.

Жүйені сегменттерге бөлу үшін мосттар мен коммутаторлар қолданылады. Олар сегменттің ішіндегі локалды трафикті сыртқа ешқандай кадрларды бермей экрандайды, тек қана басқа сегменттерде орналасқан компьютерлерге арналған кадрлардан басқа. Сонда жүйе бірнеше жүйелерге бөлінеді. Ол бір топтың ішіндегі трафиктің жиілігін және топтардың арасындағы алмасудың активтігін ескере отырып байланыс бөлімдерінің өткізу мүмкіндігін рационалды түрде таңдау мүмкіндігін тудырады.

Бір жағынан жүйенің мосттардың арасында орналасқан логикалық сегменттері бір-бірінен дұрыс оқшауланбаған, өйткені олар кеңдік толқындарынан қорғалмаған. Егер қандай да бір станция кеңдік толқындары арқылы мәліметтерді жіберсе, онда ол мәліметтер жүйенің станцияларының барлық логикалық сегменттеріне беріледі. Мосттардың көмегімен салынған кеңдік толқындарынан қорғану үшін: администратор тек бір түйінге генерирлеуге рұқсат етілген кеңдік толқындарының пакетін шектейді.

Екінші жағынан коммутаторда жасалған локалды жүйелердің виртуалды сегменттердің механизмдерін пайдалану трафиктің толық локалдауына әкеліп соғады. Ондай сегменттер бір-бірінен толық оқшауланған. Сонда мосттар мен коммутаторлардың көмегімен салынған жүйелердегі әртүрлі виртуалды сегменттерге жататын компьютерлер біркелкі жүйені құрамайды.

Мосттармен коммутаторлардың келтірілген кемшіліктері олардың каналдық деңгейлердің протоколдарымен жұмыс істеуіне байланысты. Ол протоколдарда үлкен жүйені құрылымдау кезінде пайдалануға болатын жүйенің бөлігі немесе сегментті анықталмайды. Жүйелік технологияларды жобалаушылар каналдық деңгейлерді жетілдірудің орнына ол есепті жүйелік деңгейлерге жүктеді.

Қолданушылардың көп бөлігінде жоғарғы жылдамдықпен желіге кіру мүмкіндіктері провайдерге қарағанда жоқ. Абонентпен провайдердің болу нүктесі арасындағы болатын байланыс технологиясы *технологияның соңғы милясы деп аталады*. Бұл атау шартты түрде, ал практика жүзінде осы айтылған қашықтық бір миляға сәйкес келу қажет емес. Көп жағдайларда «соңғы миля» желіден компьютер қолданушысына ақпаратты жіберу тар жол болады. Интернетке жіберу соңғы миля технологиясы әртүрлі бола алады, бірақ «кіру жылдамдығы жоғары болған сайын, каналдарды қолдану ақысы жоғары болады» деген принцип әмбебапты болып келеді. Барлық инфраструктураны қолдануға мүмкіндік беретін көптеген технологиялар бар, олар - Интернетке кіру мүмкіндігіне арналған телефонды линиялар, кабельді теледидар желілері және басқалар.

Интернетке кіру әртүрлі технологиялары: телефондық линия арқылы модеммен қосылу, радиоканал арқылы қосылу, кабельді теледидардың желісімен қосылу және де спутникті канал көмегімен қосылу. Интернетке қосылудың әртүрлі әдістеріне қарамастан, қолданушы үшін тек қосылу тұрақтылығы, мәліметтерді жіберу жылдамдығы және жауап беру уақытында ерекшеліктер бар. Интернеттің барлық ресурстарына кіруге мүмкіншілік бар. Желіге қосылудың әртүрлі нұсқаларын қарастырайық.

Интернетке кірудің әртүрлі нұсқалары. Коммутаторлық телефон линиясы арқылы қосылу. Коммутативті телефонды линияның модем арқылы қосылуы – бұл әзірше үйдегі Интернет қолданушылардың ТМД-ға таралған қосылу әдісі.

Желінің коммутациялы каналдарымен. Коммутациялы телефонды желінің немесе желінің коммутациялы каналдарымен жұмыс принципін айтайық. Сіз біреуге қоңырау шалған кезде, сіздің аралығыңызда белгілі бір физикалық байланыс каналы орналасады, олар коммутатор арқылы байланысатын жеке учаскелерден тұрады. Абоненттің әрбір учаскесі бірінші коммутаторға дейін бөлінбейтін болып келеді. Яғни, әрбір абонент осы учаскелерді жеке өзі қолданады. Желілердің қалған учаскелері коммутатор арасында ажыратылған болып келеді, дәлірек айтқанда әртүрлі уақытта әртүрлі қолданушылармен қолданылады. Бірақ, егер қайсыбір учаскелер бір қолданушымен бос емес болса, онда келесі біреу оны осы уақытта қолдана алмайды. Коммутативті телефонды линиямен қосылу - бұл уақытша (сеансты) қосылу дейді. Телефонды линия телефонды әңгімемен немесе мәліметтерді модем арқылы жіберумен бос болмауы мүмкін. «Модем» сөзі «МОДулятор» және «ДЕМОдулятор» деген сөздерден құралады. Модем телефонды линия арқылы мәліметтерді жіберуде қолданылады. Жалпы жоспарда *модем* - бұл қондырғы, цифрлық кодты әртүрлі екі жиілік дыбыстардың ауысу мен кері қайту – дыбыс тербелісін цифрлық ақпаратқа ауыстырады. Екі модем қосылғаннан кейін модулятор тұрақты тербеліс периодының басты сигналымен генерацияланады және болып жатқанды өзгертіп екінші сигналды қосады. Сонымен, жүріп жатқанның бір параметрі жіберу сигналының өзгеруіне байланысты. Демодулятор сараптама жасайды, түсетін сигнал жүріп жатқан сигналдан қалай ерекшеленеді де басты сигналды қалыптастырады. Басқаша айтқанда, жіберуші модем болып жатқан жиілікті пайдалы сигналмен моделдейді және жоғары жиіліктегі сигналды жібереді, ал модем-адресат сигналды ASCII кодына (American Standard Code for Information Interchange – ақпараттармен алмасудың стандартты коды – машиналық көріністегі латын алфавитінің әріптері, сандар мен басқа символдардан тұратын 128 код символ топтамасы, олардың әрбіреуіне 7-биттік екілік сан. Сегізінші бит жіберу кодының дұрыс контроліне жұмыс жасайды) сәйкес кері цифрлы формаға демодулейді.

Бірінші модемдер Bell Laboratories зертханалық центрінде өңделген және Bell 103 атауын алды. Бұл қондырғылар екі сыңарлы жиілікті

қолданады: сыңарлы жиілік бір модемге және сыңарлы жиілік екінші модемге. Жіберуші модем 1,07-1,27 кГц арасындағы жиіліктерге ауысу арқылы, ал жауап беруші модем 2,025-2,225 кГц арасындағы жиілікте мәліметтерді жібереді.

Bell 103 модемдері 300 бит/с жылдамдықпен жұмыс істейді, солай минутына 30-ға жуық символ жіберуге болады. Мұндай жылдамдық тек қана мәтіндік хаттамалармен алмасқан кезде қолайлы, себебі бұл жылдамдық адамның оқу жылдамдығымен салыстырғанда әлдеқайда артық. Мәліметтерді 300 бит/с жіберетін модемдер 1980 жылға дейін өмір сүрді. Сөйтсе де, адамдар суреттерді жібере бастағалы ондай жылдамдық аздау екені айқындалды.

Осы заманғы модемдер – бұл өте күрделі схемалы модуляцияларды қолданып, мәліметтерді жіберер кезде қаптайтын күрделі құрылғылар болып келеді. Клиенттік компьютер коммуникациондық портқа ноль мен бірдің реттелген түрге келтіріп, әртүрлі командалар мен мәліметтерді жібереді. Модем мәліметтерді қабылдап, оларды командалар және ақпаратқа ажыратады да, телефон линиясы арқылы жіберіп жүзеге асырады.

Қолданушы модем арқылы телефондық желіге ортақ қолданумен қосылып, ал ISP, басқа модеммен, цифрлық сигнал арқылы Интернетпен қосылады.

Бүгінгі күнгі модемдер екі түрлі: ішкі және сыртқы. Ішкі модемдер кеңелмелі плата арқылы жұмыс істесе, сыртқылары бөлек құрылғы ретінде автономды блок питаниямен істейді.

Модем (ағылш. *modem, modulator-demodulator*) — сандық сигналдарды аналогтық сигналдарға айналдыратын және керісінше амал жасайтын электрондық құрылғы.

Деректерді әртүрлі арқаулар арқылы, мысалы телефон сымы арқылы немесе радиосигналдар түрінде беруге болады. Телефон сымы арқылы аналогтық сигналдар деп аталатын импульстарды беруге болады. Аналогтық сигналдар шуыл немесе электрлік-магнитті импульстар түріндегі кедергілердің әсеріне ұшырауы мүмкін.

Дыбыстық сигналдар дерек берудің едәуір жаңа әдісі болып табылады, онда дерек беру және қабылдау үшін екілікті пішім қолданылады (нөлдер мен бірліктер тізбегімен жұмыс істейтін кодтау/кодты ағыту жүйесі). Дерек беру мен қабылдау үшін компьютерлерде дәл осы пішім қолданылады. Алайда сандық сигналдарды телефон желісі арқылы беру мүмкін емес. Сондықтан телефон сымы арқылы дыбыстық сигналдарды берер алдында оларды аналогтық сигналдарға айналдыру керек. Және тиісінше деректі қабылдаушы жақ алынған деректі сандық сигналдарға айналдыруға тиіс. Модем осындай айналдыруды жүзеге асырады – сандық пішімнен аналогтық пішімге және керісінше.

Басқа компьютерге хабар жіберу кезінде модем шығару құрылғысы ролін атқарады. Ал сіздің компьютеріңізге хабар келген кезде, модем енгізу құрылғысы ретінде жұмыс істейді. Модем сыртқы немесе жүйелік блокқа

кірістірілген болуы мүмкін. *Сыртқы модемдер* – бұл сым арқылы жүйелік блокқа қосылатын модемдер.

Модемдер сондай-ақ компьютердің жүйелік блогына кіріктірілген болуы мүмкін. Мұндай модемдер *ішкі модемдер* деп аталады

Бақылау сұрақтары:

- 1) Интернет технологиясында соңғы миля нені білдіреді?
- 2) Модем функциясы қандай?
- 3) ASCII-кодировкасы?
- 4) Модем жылдамдықтары қандай?

4 Дәріс №4. Интернет жүйесіне қатынасу технологиялары. DSL, ISDN технологиялары

Дәрістің мақсаты: Интернет жүйесіне қатынас жасау технологияларымен танысу.

Дәрістің мазмұны: DSL, ISDN технологиялары, Асимметриялы DSL (ADSL).

DSL-технологиялары.

Қарапайым телефон тек төменгі жиіліктегі желілерді қолданады. Егер «телефонды» жіңішке жолының орнына кеңірек жолды қолданса, телефон сымы едәуір көп ақпарат жібере алады. *Өткізу жолы* немесе *өткізу жолының ені* - өткізу каналы жиіліктерінің диапазонындағы ең жоғары жиілік пен ең төменгі жиіліктің арасындағы айырымы. Телефон желісі арқылы сигналды жіберудің аналогты түрі 300 Гц-тен 3,4 кГц-ке дейінгі диапазонды алады. Цифрлы сигнал үлкендеу диапазонды талап етеді. Жіберу жылдамдығы өскен сайын, жиіліктер диапазоны да өсу керек. Сондықтан, «өткізу жолы» терминімен компьютер желісімен мәліметтерді жіберу жылдамдығының жоғары шекарасы белгіленеді. *«Кеңжолды қатынас»* термині арна ақпарат жіберу үшін кеңейтілген жиіліктер жолын береді дегенді білдіреді. Ақпаратты жіберудің жоғары жылдамдығы кең жолды пайдаланған кезде бірнеше сигнал бір арнаның бойымен, бірақ әртүрлі жиіліктерде параллельді жіберілу мүмкіндігіне байланысты. Өйткені, уақыт бірлігінде ақпараттың мол көлемі жіберіледі. Арнаны бірнеше бөлікке бөліп, сигналдарды жіберу *мультиплексорлау* деп аталады. «Таржолды қатынас» терминімен дауысты жіберуге жеткілікті арна түсіндіріледі. Кейде «кеңжолды емес қатынас» термині кездеседі. Ол арнамен мәліметтерді жіберу жылдамдығы 64 Кбит/с-тан кем екендігін білдіреді.

Телефон желісін цифрлы мәліметтерді жоғары жылдамдықта жіберу үшін қолдануға мүмкіндік беретін технологиялардың бірі DSL. DSL аббревиатурасы - «Digital Subscriber Line». Бұл технология телефонмен

сөйлесуге кедергі жасамай, мәліметтерді жіберуге жоғары жиіліктерді қолдануға мүмкіндік жасайды.

DSL-технологиясы көмегімен бір уақытта Интернетпен жұмыс істеу және телефонмен пайдалануға болады. Қарапайым модемге қарағанда, DSL-қосылу жылдамдығы едәуір жоғары. DSL үшін жаңадан сымдар жүргізу керек емес, өйткені телефон желісінің құрылғылары пайдаланылады.

Асимметриялы DSL (ADSL).

Интернетпен жұмыс кезінде ақпараттың негізгі ағыны Желіден пайдаланушыға өтеді. Желіге ақпараттың едәуір аз көлемі жіберіледі. Мысалы, сіз Web-беттерді қараған кезде, кішігірім сұраныс жібересіз, ал желіден мәтін ғана емес, сонымен қатар суреттерді де қабылдайсыз. Яғни, ақпарат алмасу асимметриялы болып келеді. Бұндай трафикті жіберу үшін асимметриялы арна керек. ADSL (Asymmetrical Digital Subscriber Line) немесе асимметриялы DSL пайдаланушыға мәліметтерді жоғары жылдамдықпен жіберуге мүмкіндік береді, сондай-ақ пайдаланушыдан желіге келген сигнал желіден пайдаланушыға келген сигналға қарағанда төменгі жиіліктерде жіберіледі.

Ең жаңа технологияларды пайдалануға байланысты ADSL бойынша ақпаратты жіберу жылдамдығы басқа қатынас түрлерімен салыстырғанда өте жоғары: 8 Мбит/с абонентке бағытталғанда, 1 Мбит/с абоненттен желіге бағытталғанда. Жоғары жылдамдық Web-сайттармен, мультимедиа-ақпаратпен ыңғайлы жұмыс істеуге, үлкен файлдарды жылдам тасымалдауға және интерактивті қосымшаларды толық пайдалануға мүмкіндік жасайды.

ADSL артықшылығы болып орнатылуының жеңілдігі табылады: пайдаланушы мен телефон компаниясын бірімен-бірін қосатын бұрыннан бар телефон кабелінің сымдары қолданылады. ADSL Интернетке үнемі қатынасты қамтамасыз еткеннің өзінде ADSL пайдаланушылары өткізу жолын басқа абоненттермен бөліспейді. Бірақ ADSL кемшіліктері де бар, ең алдыңғысы – алыстықтың шектелуі. ADSL-технологиясын қолданған кезде кері бағытта ақпаратты жіберу жылдамдығы ара қашықтыққа байланысты болады. Егер абонентке бағытталған ақпаратты 3 км қашықтықта 8 Мбит/с жылдамдықпен алуға болса, 5 км қашықтықта – тек 1,5 Мбит/с.

Пайдаланушы ДК-і ADSL-модемге қосылады. ADSL-модемді жұмысының принципі 24 кГц-тен 1100 кГц-ке дейінгі жиіліктер диапазоны әрқайсысына виртуалды модем бекітілетін 4000-герцтік жолдарға бөлінетіндігіне негізделген. Соған байланысты виртуалды модемдердің әрқайсысы өз жиіліктер диапазонымен жұмыс істейді.

ADSL – модемі жиілікті айырымға қосылады. Жиілікті айырым (немесе сплиттер) кәдімгі телефон байланысының төменгі жиілікті сигналы мен жоғары жиілікті ADSL-сигналын айыратын төменгі жиіліктердің фильтрі болып табылады. Жиілікті айырым үш ұяшыққа ие блок түрінде жұмыс істейді: біреуі - ADSL-модемге қосылуы үшін, екіншісі – телефон

құрылғыларына қосылуы үшін, үшіншісі – ADSL желісіне қосылу үшін. Жиілікті айырым бір желіге телефонды да, компьютерді де қосуға мүмкіндік береді. Телефон станциясындағы дәл сондай жиілікті айырым абоненттік сымның басқа жағында жоғары және төменгі жиілікті сигналдарды бөледі.

Дыбысты сигнал телефонды желіге, ал цифрлы сигнал DSLAM (Digital Subscriber Line Access Multiplexer) қатынас мультиплексорына бағытталады. Бұдан провайдер желісі арқылы Интернетке өтеді.

Қатынас мультиплексоры – барлық DSL-абоненттерін бір жоғары жылдамдықты желіге қосатын, телефон компаниясының ғимаратында орнатылған механизм.

ADSL – экономды технология. Қарапайым жағдайда аналогты өткізу қабілеті бар бөлінген арнаға қарағанда, желі пайдаланушыға арзан түседі.

ISDN-технологиясы.

Бөлінген телефонды желі – екі абонентті үнемі қосатын телефонды байланыс желісі. Бөлінген желінің едәуір таралған технологиясы болып ISDN (Integrated Services Digital Network) табылады. *ISDN* – ақпаратты жіберудің цифрлы түрінің стандарты. *ISDN*-желісінің негізгі компоненті - 64 Кбит/с өткізу қабілеттілігі бар бір бағытталған bearer-арнасы немесе В-арна. Бұл арнамен цифрлы ақпарат жіберіле алады. Өткізу жолын кеңейту үшін В-арналар екі-екіден топтасады да, арналар тобына ақпарат алмасуды басқаратын D-арнасы (16 Кбит/с) қосылады. Ақпарат алмасу кәдімгі мыс сымның көмегімен атқарылады. Модемнің орнына ISDN-адаптерді орнатқан пайдаланушылар 128 Кбит/с дейін баратын жылдамдықтағы Интернетке қол жеткізе алады.

ISDN-адаптерлерін кейде ISDN-модемдері деп атайды. Бұл терминді дұрыс деуге болмайды, өйткені ISDN-адаптерлер модуляция және демодуляция функцияларын атқармайды, ISDN-желісі алдынан-ақ цифрлы болып табылған. ISDN-арнасын телефон компаниясы береді. ISDN-желісімен телефонмен сөйлесу және сол уақытта Интернетке ақпарат жіберуге болады.

Төменде әртүрлі технологиялар бойынша Интернетке қатынарудың максималды жылдамдықтары келтірілген.

Қатынасу технологиясы	Максималды жылдамдық
Коммутирленетін телефондық линия	56 Кбит/с
ISDN	128 Кбит/с

Кабельді телевидение	36 Мбит/с
ADSL 2	1 Мбит/с (запрос), 10 Мбит/с (жауап)
2,4 ГГц диапазонындағы радиоарна	До 54 Мбит/с
Серікті қатынас	Жүйеге байланысты бірнеше Мбит/с
T1	1,544 Мбит/с
T3	44,74 Мбит/с
GSM-data	9,6 Кбит/с
GPRS	160 Кбит/с (теоретикалық максимум)
UMTS	2,048 Мбит/с

Бақылау сұрақтары:

- 1) DSL – технологиясымен ақпаратты жіберудің ерекшелігі неде?
- 2) ISDN– технологиясымен ақпаратты жіберудің ерекшелігі неде?
- 3) ADSL – технологиясымен ақпаратты жіберудің ерекшелігі неде?
- 4) ISDN және DSL технологияларын қолдану үшін қандай құрылғы қажет?

5 Дәріс №5. Интернеттегі web серверлер. Web – сервер жұмысының механизмі. Статистикалық және динамикалық беттер. CGI технологиясы. Скриптер

Дәрістің мақсаты: интернеттегі web-серверлер жұмысының механизмімен, функцияларымен, статистикалық және динамикалық web-беттермен, CGI технологиясымен танысу.

Дәрістің мазмұны: статистикалық және динамикалық беттер. CGI-технологиясы. Скрипт программа.

Web-сервердің функциялары.

Web-сервердің басты тапсырмасы қолданушылардан НТТР-сұраныс қабылдау, сұраныстарды өңдеу және оларды сандық компьютерлік кодқа айналдыру. Содан кейін, НТТР-жауапты миллиондаған нөлдер мен бірлерді кескінге, медиа-ағынға, әріптерге, HTML парақтарға айналдырады.

Кез келген веб сервер қолданушыға ыңғайлы болатындай веб браузері болғаны дұрыс. Ол веб серверге интернет ресурстардың URL-адресқа өзгертілген сұраныстарды жібереді.

Стандартты функциялармен қатар, кейбір веб серверлердің қосымшалары болады. Мысалға алатын болсақ, сәйкес келетін программалық қамтамалар ресурсқа қолданушының қатынас жасауын бақылап отырып, оларды жеке журналға жазуы мүмкін. Көп жағдайда веб сервер мэйл сервермен бірге орнатылады. Бұл қолданушыларға сайттың өзінен тікелей, бір ғана гиперсілтемені баса отырып поштаның бетіне тез арада өтуге мүмкіндік береді.

Веб сервер не үшін қажет?

Жоғарыда атап өткендей, веб сервер ақпарат алмасу үшін Интернет желісін қолданатын барлық қолданушылар үшін қажет. Дегенмен, көп мөлшерде оған қатынас жасайтын адам емес, программалар мен құрылғылар. Мысалы, антивирустық программалар серверден желіден іздеуді және өзінің мәліметтер базасын жаңартуды сұрайды. Веб серверлермен белсенді жұмыс жасайтын ұялы телефондар, теледидарлар, Интернетке қатынас жасай алатын басқа да құрылғылар. Программаларды автоматты жаңартуға баптауға болады. Бұл жағдайда қолданушының қажеттілігі болмайды. Кейбір жаңартылатын мәліметтер базасын жеке түрде қадағалап отырғаны дұрыс.

Ең танымал веб серверлер.

Атақты және кең таралған веб серверлар болып Microsoft IIS және Apache табылады. Осылардың арасында ең танымалы Apache. Оның программалық қамтамасы барлық бар болатындардың ішінен 60% қолданылады. Көп жағдайда бұл мүмкіндік Apache серверінің тегін болуына байланысты. Өндірушілер күнделікті өздерінің өніміндегі қателіктерін ретке келтіреді. Бұл программаның кемшілігі мамандандырылған программистер мен қолданушыларға арналған, сол себептен де болар қызмет көрсету және баптау біршама күрделі.

Microsoft компаниясы, керісінше, өзінің IIS веб серверін түсінуге қолайлы болатындай етіп, ортастатистикалық қолданушыларға дайындауға тырысып жатыр. Олардың баптауын мамандардың көмегінсіз жүргізуге болады.

Apache де, IIS де көптеген операциялық жүйелермен жақсы жұмыс жасайды. Мысалы, Mac OS, Linux, Microsoft Windows түрлі модификациясымен және т.б. көптеген түрлерімен. Бұл екі сервер жұмыс жасағанда ыңғайлы, жылдамдығы жақсы, оларға қосымша модульдерді қосуға болады.

Браузердің адрестік жолындағы қажетті URL-ді теріп болған соң, браузер пайдаланған протокол (HTTP) жөнінде мәлімет және сервер атын алады. Сервер атын IP- адреске ауыстыру үшін браузер DNS серверіне жүгінеді. Алынған IP- адрес негізінде браузер ізделінді Web- сервермен байланыс орнатады және HTTP протоколын пайдалана отырып ізделінді ресурсты сұрайды. Сервер браузерге серверде сақталатын HTML бетін жібереді. Браузер HTML- тәгтерін оқу нәтижесінде сіздің компьютеріңіздің экранында бет ашалады, одан сіз өз сұранысыңыздың нәтижесін көре аласыз. Әдетте қарапайым Web беттерде тек текст қана емес графиктерден де тұрады, яғни әртүрлі типтегі бірнеше файлдан тұрады. Браузер ол файлдарды тану үшін, сервер қандай файлды (HTML форматындағы текст немесе JPG форматындағы графика және т.б) жіберу керек жөнінде мәлімет береді, содан соң файл мазмұны жіберіледі. Әдетте, Web беттер көптеген файлдардан тұрғанына қарамастан бір рет сұраныс уақытысында Web сервер тек қана бір файлды жібереді. Яғни, html текст алып одан

графикалық элементке сілтеме тауып, браузер серверге жаңа сұраныс жібереді (html текст келген серверге ғана жіберу міндетті емес). Әрбір жаңа файлды көшіріп алу үшін браузер жаңа HTTP сұранысын жіберу керек. Бұнда қазіргі серверлермен браузерлер көп ағынды режимде жұмыс істейтіндіктен бір мезгілде бірнеше сұраныс орындалуы мүмкін. Егер берілген адреске сұранып отырған ресурс жоқ болса онда Web сервер мынандай мәлімет береді: *404/File not found (файл табылмады)*.

Статистикалық және динамикалық беттер.

Статистикалық беттер Web сервер каталогында орналасқан файлдардың нақ копиясы болып табылады және өңдеуші өзі онда бір нәрсені ауыстырмайынша өзгермейді. Дегенмен беттер динамикалық түрде қалыптасады, яғни дискідегі дайын файлан емес, белгілі бір программада сұраныстың өңделу уақытында. Осындай беттердің қалыптасуының бірнеше әдістері бар.

Тікелей Web серверде сұранысқа сәйкес қалыптастыру.

Web беттерді динамикалық қалыптастырудың мүмкіндігін жүзеге асыру үшін серверге мынадай бағыт берілуі керек, қандай файлдар «кәдімгі» болады, ал қандайы оның программалық өңделуіне нұсқаулары болады. Бұл жағдайда бетті сервердің өзі құрастырады (арнайы командалар көмегімен немесе ішкі бағдарлама). Беттердің динамикалық қалыптастыратын командасы болатын программа мәтіні *скрипт* деп аталады.

Тұтынушы компьютерінде қалыптастыру.

Бұл жағдайда программа мәтіні динамикалық web- парағын қалыптастыру үшін алдымен тұтынушының локальдық компьютеріне беріледі, бұнда браузер web- парағын алу және өңдеу үшін оған сәйкес заттар шақыру керек. Динамикалық беттерді қалыптастыру үшін бірнеше технологиялар бар.

CGI- технологиясы.

Біздің сұранысымызға сәйкес дайындалған динамикалық беттер «жылдам қалыптасты». Мысалы кез-келген пікірлер кітабы сізге белгілі бір форманы көрсетеді, мұнда сіз өз мәтініңізді қосасыз, келесіде осы бетті ашсаңыз онда жаңа хабарлама тұрады. Web-парағына динамикалық мазмұнды қосуға мүмкіндік жасайтын технологиялардың бірі CGI (Comman Gateway Interface) болып табылады. Ол сол немесе басқа URL мен статистикалық документі емес программаны түсінуге мүмкіндік жасайды нәтижесінде нақты уақытта мәліметтер қалыптастырады. Мысалы егер сіз белгілі бір аймақтағы ауа райының сол кездегі мәліметін бергіңіз келсе, онда сіз әр бір ретте жаңа бетті құруыңыз керек. Бұл CGI технологиясының негізінде жүзеге асыруы мүмкін. Серверде жұмыс істеу бастағанда CGI программасы қосылады, ол цифрлы өлшеуіш құралына айналып температура, қысым және т.б мәліметтер береді. Әр кезде осы адрестен мәлімет алу үшін байланысқаныңызда сіз сол уақыттағы мәліметті аласыз. Басқа мысал: егер сіз ізденіс жүйесінен белгілі мәлімет алғыңыз келсе онда

CGI программасы жұмысының нәтижесін ізделінді адресстер жиынтығы түрінде аласыз.

CGI программасын нақты уақыттағы Web сервердің бір бөлігі ретінде қарастыруға болады. Сервер тұтынушының сұрағын CGI программасына береді, ол оларды өңдеп жұмыс нәтижесін тұтынушы экранына қайтарып береді. Клиент үшін адрессте URL статистикалық құжат па немесе CGI программа ма еш қандай айырмашылығы жоқ. CGI программалары жұмысының нәтижесі статистикалық құжат сияқты форматта болады. CGI терминін тек қана программа емес протокол ретін де түсінуге болады. Бұл жағдайда CGI Web сервер үшін стандартты тәсіл болып табылады– тұтынушы сұранысын бағдарламаға беру және одан мәлімет алу. Сервер мен оның қосымшасының арасындағы бір біріне мәлімет жіберу жөніндегі CGI протоколы HTTP протоколының бір бөлігі болып табылады. CGI программасының үлкен бөлігі CGI скрипталары болып табылады. Скрип дегеніміз интерпритацияланатын немесе басқа программаларымен жұмыс жасайтын ережелер жинағы. Perl, JavaScript тілдері тура осы скрипталық тілдер түрінде ойлап табылған. Олар сценарийлер жазу тілдері деп те аталады. Негізінен CGI программасы скрипттік тілде және де компилярлық тілде жазылуы мүмкін. C, C++, Delphi.

CGI альтернативті технологиясы Microsoft компаниясының технологиясы болып табылады. Ол былай аталады Active Server Page (ASP) ол да сол принциппен құрылған: web-серверге қосылған скрипт, парақ тұтынушыға жіберуден бұрын серверде орындалады. Осы принциппен орындалатын басқа да бір қатар технологиялар бар. Динамикалық мазмұны сервер жағындағы қалыптасатын схемадан өзгеше динамикалық мазмұны тұтынушы жағында көрінеді. Соңғы жағдайда активті құжаттар web серверде және локальдік компьютерде сақталады. Онда белгілі бір есептеулер орындалады және осы есептеулер нәтижесі экранда көрсетіледі. Активті құжаттарды дайындауда түрлі технологиялар пайдаланады: бұл мәліметтер JavaScript те Java апплеттерде жазылған қосымша болуы мүмкін және басқару элементі ActiveX болады.

Бақылау сұрақтары:

- 1) Web-сервер жұмысының механизмі қандай?
- 2) Ститистикалық және динамикалық беттердің айырмашылығы?
- 3) CGI, ASP серверлерінің технологияларының айырмашылығы неде?
- 4) «Скрипт программа» ұғымы нені білдіреді?

6 Дәріс №6. Web-ресурстарды алу технологиясы. Web-парақтарды кэштеу. Прокси-сервер механизмінің жұмысы

Дәрістің мақсаты: web-ресурстарды алу технологиясымен танысу, web-парақтарды кәштеу.

Дәрістің мазмұны: web-парақтарды кәштеу. Прокси-сервер. Құжаттардың жарамдылық мерзімі. WEB-жылдамдатқыштары. Кәштеу процесін оптимизациялау арқылы жылдамдату. Индексті құру. Домендік атты теру. Сілтемелердің тематикалық жинағы. Индекстелген каталогтер.

Web-парақтарды кәштеу.

Егер сервер үлкен жойылуда болса, Интернетке шығу жылдамдығы төмен болса немесе қайта қосылу режимінде жұмыс істесе, көбінесе ақпарат кешіктіріліп беріледі. Бұл кезде қосылуды жылдамдату сұрағы туындайды. Осы сұрақты шешудің бір жолы, мәліметтерді жойылған серверлерден бірнеше рет алуға болмауында. Web навигациясы кезінде көбінесе кітаптағындай «парақты артқа парақтау» сияқты, яғни параққа қайта қосылу қажеттілігі туындайды. Браузерде *Артқа* пернесін басып, алдында көріп өткен параққа қайта оралғанда, оны серверден қайта алудың мағынасы жоқ екені анық. Сондықтан көріп өткен құжатты компьютердің дискінің арнайы буферлік аймағында (кәште) сақтаса, қолданушының қайта оралғысы келген жағдайда сілтемені тез ашып көруге мүмкіндігі болады. Қазіргі заманға сай браузерлер дәл осылай жұмыс жасайды. Мәселен, сіз парақтарды 1-2-3 кезегімен қарап, 3-ші парақ 4-ге ссылқасы бар деп ойлайық. Осы жағдайда 3-ші парақтан 4-ге өтумен (Жүйеден жүктеу) салыстырғанда 2-ге өту тез (кәштан жүктеу) орындалады.

Қазіргі заманға сай браузерлерде (Internet Explorer және Netscape Navigator) кәштелген құжаттарды сақтау үшін папканың көлемін өзгерту мүмкіндігі бар.

Прокси-сервер.

Кәштеу технологиясында өзінің шектеулері бар. Мысалы, сіз және сіздің әріптесіңіз Интернетке бір провайдер арқылы қосылған болсаңыз. Бір кезде сіз, алдында сіздің әріптесіңіз алған құжатты сол провайдердің каналынан сұрайсыз. Жүйеден қайта-қайта бір құжатты сұрау дұрыс емес. Мәліметтерді сервер провайдер деңгейінде кәштау дұрыс.

Бұл мәселені шешу провайдерлер прокси-серверге (ағылшынның *проху*-орынбасар деген сөзінен) жүктейді. *Прокси-сервер* – бұл қауіпсіздікті, әкімшілік бақылауды және кәштау функцияларын жоғарылатуға мүмкіндік беретін, қолданушының жұмыс станциясы мен Интернет арасындағы посредник ролін атқаратын сервер.

Прокси-сервер қолданушыдан қандай да бір интернет-сервисті орындауға сұраныс алады, мысалы, web-парақты көріп өтуге сұраныс. Егер прокси кәштау функциясын орындаса, ол сервердің локальді кәшінде сұрап отырған парақтың жоқтығын қарайды. Егер бұл парақ бар болса, ол қолданушыға сұраныс Интернетке берілмей қайтарылады. Ал, егер кәшта бұл парақ болмаса, прокси-сервер клиент ролінде қолданушының атынан, өзінің IP-адресін қолданып, Интернеттен керек параққа сұраныс жібереді.

Парақ қайта оралғанда, прокси-сервер оны қолданушыға жібереді. Прокси-сервердің кэштау функциясы Интернетпен жұмысты едәуір жылдамдата алады және жүйелік трафиктің көлемін азайта алады. Web-парақтарды кэштеу Жүйенің жұмысын жақсартудың бір жолы болып табылады, себебі ол web-түйіннің уақытты бұзылыстарын қалыпқа келтіреді.

Әдетте, прокси-сервер программасы жұмыс істейтін компьютерде едәуір дисктік аула бөлінеді. Үлкен провайдерлер құжаттарды кэштеуге ондаған және жүздеген гигабайт жады бөле алады.

Осылайша, үнемі ізделіп отыратын құжат тек құжатты шығарушының серверінде ғана сақталып қоймай, сонымен қатар «қолданушыға жақынырақ», провайдер прокси-серверінде немесе қолданушының өз компьютерінде сақтала алатындықтан, іздеген құжаттарды тез көре алу мүмкіндігі бар.

Біз мыңдаған клиенттері бар провайдерлер жөнінде айтқана, жүйедегі құжаттардың белгілі бір бөлігін ғана сұрайтынын айтып өткен жөн. Мыңдаған клиенттермен жұмыс істейтін үлкен ISP-дің прокси-сервері, сұраныстардың 50%-ға жуығын өз дискінен орындайды. Әдетте ISP сервері регионның басқа интернет провайдерлердің серверлерімен байланысты. Сондықтан, егер клиентті қызықтырып отырған құжат провайдердің прокси-сервер кэшінде табылмаса, ол басқа прокси-серверлерде табылуы мүмкін. Осылайша, кэш-ауласындағы қолданушылардың көлемі көп есе көбейеді.

Құжаттардың жарамдылық мерзімі.

Ескірген кэштелген файлды алмау үшін, кэштелген құжаттарды қашан сұранысқа қоюға болады, ал қашан қоюға болмайтығын анықтайтын бірнеше ережелер бар. Бұл ережелердің бір бөлігі HTTP протоколында жазылып өткен, ал қалғаны браузер баптауында және прокси-сервер әкімшілігімен ұсынады. Прокси-серверде кэштеуге шешім қабылдаудың бірнеше критерилері бар. Мысалы, егер объект жасырын болса, ол кэштелмейді. Сол сияқты кэштелген құжатты клиенттің сұранысы бойынша жіберіле алуға шешім қабылданатын критерилер бар. Мысалы, егер құжаттың жарамдылық мерзімі өткен болса, онда сервер оны клиентке жібермей, сайтты құрастырушының серверінде жаңалау құжаттың бар, жоқтығын сұрайды. Жарамдылық мерзімі өтіп кеткен құжат жай жаңартылмаған, яғни ескірмеген болуы мүмкін және оны клиенттің сұранысына беруге болады.

Web-жылдамдатқыштары.

Стандартты браузерлер кэштеу технологиясын Web-парақтарды жүктеуді жылдамдату үшін қолданатынын айтып кеткен болатынбыз. Бірақ, жүктеу процесін Internet Explorer-ға қарағанда жақсырық орындайтын арнайы программалар бар. Жылдамдату жүйелік қосылулардың параметрлерін оптимизациялау арқылы, мәліметтерді кэштеу және «қажеті жоқ» мәліметтерді алып тастау арқылы жүзеге асыруға болады. Кейбір

программаларда жоғарыда айтып өткен механизмдердің бірден бірнешеуі жүзеге асырылған.

Кэштеу процесін оптимизациялау арқылы жылдамдату.

Мәліметтерді кэштеу кезінде Web-парақтарды жүктеуді жылдамдатуды айтқанда келесі бағыттарды белгілеп өткен жөн:

- IP-адресстерді кэштеу;
- локальді компьютерде дискті кэшти оптимизациялау; Әр бағыттың неден құралғанын түсіндіріп өтейік.

Сіз URL браузерге сол немесе басқа ресурсты жібергенде, ол DNS-серверге доменді атты IP-мекенге жіберуге сұраныс жасайтыны белгілі. Қажетті мәліметтерді табу алдында қаншама DNS-серверлерді сұрап өтеді. Әдетте, IP-адрес қолданушы компьютерінде кэштелмейді және сіз бірнеше минут алдын қолданып отырған мекен қайта сұралып отырады, ол тағы да уақыт алады. Сондықтан, Web-парақтарды көрсетуді жылдамдатудың бір жолы DNS-серверлерді едәуір оптималды сұрау жүргізетін және *IP-мекендерді кэштеуді ұйымдастыратын* программаны қолдану болып табылады.

IP-мекенді алып болғаннан кейін, шолушы (обозреватель) компьютердің кэшінде көрсетілген парақ көшірмесінің сақталғандығын тексеріп, егер кэштегі құжат жарамды болса, ол қолданушыға жіберіледі. Бұл процессте уақыт алады және оны жылдамдату – бөлек мәселе, сондықтан оны басқа программаға жүктеуге болады. Осы мәселемен айналысатын көптеген программалар көп орын алатын, бірақ жылдам істейтін өз кэшін құрады. Жылдамдатудың екінші бағыты осыны құрайды.

Үшінші механизмді яғни, алдын-ала ескертілетін оқытуды (упреждающее чтение) түсіндіру үшін, кәдімгі браузердің жұмысына қайта оралайық. Құжат браузермен көрсетілгеннен кейін, әдетте үзіліс болады. Қолданушы құжатты оқығанша жүктеу процесі тоқтатылады, яғни, жүйе жұмысы тоқтап қалады. Бұл механизм үзіліс кезінде қосылыстарды қолдануға мүмкіндік береді, бұл кезде осы параққа сілтемесі бар құжаттар жүктеледі. Осы құжаттардың фондық режимде жүктелуі қолданушы сұраныс жібергенде тез көрсетуге мүмкіндік береді. Үшінші механизм осы *префетчингтан (prefetch-ағылшынның алдын-ала алып келу деген сөзінен)* құралады. Кейде осы механизмді алдын-ала ескертілетін жүктеме (ағылшынның *pre-loading* деген сөзінен) деп те атайды.

Бақылау сұрақтары:

- 1) Web-парағын кэштеу принципі неде?
- 2) Прокси-серверінің жұмыс механизмі неде?
- 3) Web-парағын кэштеу оптимизациясының механизмі қандай?
- 4) Web-парағын кэштеудің үш негізгі бағытын атаңыз?

7 Дәріс №7. Интернеттің іздеу технологиялары

Дәрістің мақсаты: қажетті ақпаратты іздеу принциптерімен, іздеу машинасының жұмыс механизмімен танысу.

Дәрістің мазмұны: қажетті ақпаратты іздеу принциптері. Іздеу машинасының жұмыс механизмі. Индексті құру.

Web-тен іздеу.

Интернетте миллиондаған сайттар бар, соның ішінде өзекті ақпаратпен қоса көптеген ескі қорлар орналыстырылған. Интернет – белгілі бір басқарушысы жоқ демократиялық ақпарат көзі болып табылады. Кез келген адам желіге өзінің қорын орналастыра алады. Қорытындылап келгенде, интернетте ақпараттың қайталанбауына, оның стандартқа сай келуіне көп адамдар мән бере бермейді. Желіде барлығы бар екені белгілі, бірақ желіден қажетті ақпаратты алу қиын. Яғни, мәліметті табу үшін, оны жақсы іздей білу керек. Осы бөлімде интернет желісімен жұмыс істейтін іздеу аспаптары сипатталып, іздеу жүйесінің жұмыс механизмі түсіндірілген, іздеу оптимизациясына практикалық түсініктеме берілген.

Интернетте ақпаратты іздеуге арналған мынадай әртүрлі аспаптар бар: іздеу машиналары (поисковиктер), индекстелген каталогтер (рубрикаторлар), рейтингілер, метаіздеуші жүйелер және тематикалық сілтемелердің тізімі, онлайн энциклопедиялары мен анықтамалар. Осы кезде әртүрлі үлгідегі ақпаратты табуда іздеу аспаптарының түрлі категорияларын қолдану тиімді болып келеді. Әр категорияны жеке қарастырайық.

Индекстелген каталогтар.

Каталог дегеніміз тақырыптары бойынша топтастырылған иерархиялық құрылым түрінде берілетін мәліметтер. Иерархиялық құрылымның бірінші деңгейіндегі тематикалық бөлімі «спорт», «демалыс», «ғылым», «дүкендер» сияқты кең тараған тақырыптардан тұрады. Ал әр бөлімнің бөлімшелері болады. Осылайша, біртіндеп каталог бұтақтары арқылы саяхат жасап, іздеу облысын кішірейте отырып, сіз өзіңізге керекті облысты дәл анықтай аласыз. Мысалы оқу орындарын іздеу барысында мынадай тізбек пайда болуы мүмкін: *Білім-> Оқу орындары -> Жоғары оқу орындары -> Институттар.*

Қажетті ішкі каталогты тапқаннан кейін, одан сілтемелер жинағын аласыз. Каталогтарды программалар емес, адамдар құрастырғандықтан, каталогтағы барлық сілтемелер профильді болып табылады. Егер сіз ортақ тақырыпта жалпы ақпарат іздесеңіз, онда каталогтарға қатынаған дұрыс. Ал егер сізге нақты бір құжатты табу керек болса, онда каталог тиімсіз іздеу құралы болып табылады.

Желіде ортақ қолданылатын каталогтардан басқа, ерекшеленген каталогтар да бар. Егер де бір каталогта өте көп қор орналасса, онда оларды кең таралуына байланысты бірнеше бөліктерге бөлуге (ражнирование) болады. Мысалы, Яндекс каталогында бөліктеу басқа сайттардың біздің сайттағы сілтемелерінің индексімен жүргізіледі.

Желіде каталогтардан басқа рейтингтер де бар. Каталогтан рейтингтің айырмашылығы, мұнда қорларды тікелей оның иесі суреттесе, ал каталогта - авторы, демек оның редакторлары суреттейді.

Сілтемелердің тематикалық жинағы.

Сілтемелердің тематикалық жинағы – бұл кәсіби топтармен немесе жеке жинақтаушылармен құрылған тізімдер. Шектелген кәсіби тақырыпты ірі каталогтің жұмыскерлер тобына қарағанда сол жұмыстың кәсіби маманы жақсы ашуы мүмкін.

Домендік атты теру.

Каталог – бұл ыңғайлы іздеу жүйесі, бірақ егер сізге Intel немесе IBM компаниясының сервері керек болса, сіз каталогке қатынай алмайсыз. Сәйкес сайттардың атын табу қиын болмайды: www.intel.com, www.ibm.com.

Сол сияқты, сізге егер ауа райына арналған сайт қажет болса, оны www.weather.com серверінен іздеген дұрыс болады. Көп жағдайларда кілттік сөз арқылы сайтты табу мәтінде көп кездесетін сөзден тұратын құжатты тапқаннан ыңғайлы.

Іздеу кезінде танымалы емес компаниялардың адресінің атын ойдан тергенде, бірде-бір іздеу жүйесінде тіркелмеген сервермен байланыс орнатуы мүмкін болғандықтан, ол іздеудің басқа түрлерімен табысты бәсекелесе алады. Осыған ұқсас іздеулер тиімсіз, сондықтан ізделінетін сайттың атын таба алмайтын болсаң, іздеу машинасын қолдану керек.

Іздеу машиналары.

Сұранысқа жауап ретінде сіз әдетте құжаттардың ұзын тізімін аласыз, оның көбі сіздің сұрағыңызға жауап бермейді және сол тақырыпқа ешқандай қатысы болмайды. Сондай құжаттар релевантты емес (ағылшын сөзінен шыққан, *relevant*- лайықты, қатысты) деп аталады, ізденіс бойынша табылған құжаттар релевантты құжаттар деп аталады.

Табылған сілтемелердің тізіміндегі релевантты құжаттардың проценті сұраныстың дұрыс қойылуына байланысты болады.

Іздеу машинасы тапқан барлық құжаттардың ішіндегі релевант құжаттардың бөлігін іздеу дәлдігі деп атайды. Релевантты емес құжаттарды шуы бар құжаттар деп атайды. Егер табылған құжаттардың барлығы релевантты болып келсе (шуы жоқ құжаттар), іздеу дәлдігі 100% құрайды. Егер барлық релевантты құжаттар табылса, онда іздеу толымдығы 100% тең.

Сайып келгенде, іздеу сапасы екі өзара тәуелді параметрлермен анықталады: дәлдікпен және іздеу толықтығымен. Толықтықтың артуы дәлдікті төмендетеді және керісінше.

Іздеу машинасының жұмыс механизмі.

Іздеу жүйелерін анықтама қызметімен салыстыруға болады, онда агенттер кәсіпорындарды аралап, мәліметтерді деректер базасына жинайды. Клиент анықтама қызметіне жолыққанда ақпарат сол деректер базасынан алынады. Мәліметтер базада ескіріп отырады, сондықтан агенттер оларды оқтын-оқтын жаңартады. Кейбір кәсіпорындар мәліметтерді өздері

жібереді, сондықтан агенттердің оларға барудың қажеті болмайды. Басқаша айтқанда, анықтама қызметінің екі функциясы болады: жасау және деректер базасын тұрақты жаңарту және клиент сұранысы бойынша базадан хабар іздеу.

Сол сияқты, іздеу машинасы да екі бөлімнен тұрады: робот – ол берілген серверлерді аралап деректер базасын қалыптастырады және іздеу механизмі. «Робот» терминінің көптеген синонимдері бар, роботтан басқа оны желілі агент немесе торапта жүргеніне байланысты құрт немесе өрмекші дейді.

Робот базасы негізі роботтың өзімен (робот өзі жаңа қорларға сілтемелер тауып алады) және аз дәрежеде өз сайттарын іздеу машиналарында тіркейтін қор иелерімен қалыптасады. Деректер базасын қалыптастыратын роботтан басқа табылған сілтемелердің рейтингісін анықтайтын программа бар.

Іздеу машинасының жұмыс принципі пайдаланушы көрсеткен кілттік сөздер арқылы ішкі каталогтан (деректер базасы) релеванттігі бойынша сұрыпталған сілтемелер тізімін беру арқылы іске асырылады.

Іздеу жүйесі тек ішкі каталогтармен операциялайтынын атап айтқан жөн. Іздеу машинасының мәліметтер базасы жүйедегі түйіндік адресстерді сұрау арқылы әрдайым жаңартылатынына қарамастан, іздеу машинасының ішкі қорларын және желі қорларын салыстыруға келмейді, сондықтан әрқашан машина ескірген адрес немесе қажетсіз ресурс табатыны өте ықтимал. Проблема тек қана ішкі қорлардың шектілігінде ғана емес, тағы роботтың жылдамдығының шектілігінде тұр. Іздеу машинасының ішкі қорларының көбеюі проблеманы шешпейді, себебі аралау жылдамдығы ақырғы болып табылады. Бірақ іздеу машинасының ішінде каталогтарға бөлінген Интернеттің кіріс қорларының белгілі бөлігінің көшірмесі болады деуге болмайды. Толық ақпарат (кіріс құжаттар) бәрі бірдей сақталмайды, көбіне жиі тек оның бөлігі – индексстенген тізім немесе индекс деп аталатын, құжат жолынан шағын бөлігі сақталады.

Индекс құрау үшін кіріс мәліметтер қор көлемі минималды, ал іздеу тез әрі максималды пайдалы ақпарат беретіндей түрлендіріледі. Индекстелген тізімді түсіндіру үшін оның қағаз аналогы – конкорданс, яғни сөздікті келтіруге болады, онда белгілі жасушымен қолданылатын сөздер алфавиттік тәртіпте болады және де жазушы шығармасында келтірілгеніне сілтеме болады.

Айтпаса да түсінікті, конкорданс (сөздік) шығарма тексінен шағын және одан керекті сөзді іздеген кітапты түгел парақтағаннан көп жеңіл.

Индексті құру.

Желілік агенттер немесе робот-өрмекшілер Желі бойымен «өрмелейді», Web – беттерді талдайды және не әрі қай парақта табылғаны туралы ақпарат жинайды. Кезекті HTML-парақтарды табысымен көптеген іздеу машиналары (әр іздеу машиналарында әртүрлі) сөздерді, суреттерді, сілтемелерді және де басқа да элементтерді белгілейді. Сөздердің парақта

барлығы ғана емес, әрі оның орналасуы, яғни бұл сөздің қайда орналасқаны: тақырыпта (title), тақырыпшаларда (subtitles), метатэгте (meta tags) немесе басқа орындарда. Әдетте негізгі сөз ескеріледі де, шылау мен одағайлар: «ал», «бірақ» және «немесе» еленбейді. Метатэгтер парақ иелерінің өзіне сол арқылы ізделінетін кілттік сөздер мен тақырыпты анықтауға мүмкіндік береді. Бұл әсіресе кілттік сөздің бірнеше мағынасы болғанда қажет. Метатэгтер іздеу машинасын сөздердің бірнеше мағынасынан дұрысын таңдауға көмектеседі. Алайда, метатэгтер адал толтырылғанда ғана сенімді жұмыс істей алады. Web-парақтардың кейбір иелері өздерінің метатэгтеріне желіде көп аталатын өз сайт тақырыбына қатысы жоқ сөздермен толтырады, сол арқылы өзінің жаңа келушілерін тарту әрі қор қатысуы рейтингісін жоғарылату үшін жасайды. Іздеуден осы сияқты сайттарды шығару – жақсы іздеу жүйесінің тағы бір тапсырмасы. Әрбір роботтың өз қараниетті жарнама үшін жазаланған қор тізімі бар.

Тапсырма берілген Web-парақтарда ақпарат жиналғаннан кейін алынған мәліметтерді индекстеу жүреді. Робот-өрмекшілер Web-парақтардың ақпараттарын қарастырып, кілттік сөздер арқылы индекстенген іздеу базасын құрады, содан кейін пайдаланушы сұранысы арқылы жүйе дұрыстығына (релевантты) қарай сайттар тізімін береді. Айқын, егер сіз сайтты «гүл» деген кілттік сөзбен іздесеңіз, онда іздеу машинасы сол сөз бар парақтарды тауып қана қоймай, бұл сөздің қай жерде сайт тақырыбына қатыстылығын анықтай алуы керек. Сөздің Web-парақтың профиліне қатыстығын анықтау үшін оның парақта қаншалықты жиі ұшырасатынын, берілген сөз туралы сілтемелердің бар-жоқтығын бағалау керек. Қысқаша айтқанда, парақта табылған сөздерді маңыздылық дәрежесіне қарай рангілеу керек.

Сөздерге салмақтылық коэффициенттері оның қанша және қайда кездесетініне қарай (парақ тақырыбында, беттің басы не аяғында, сілтемеде, метатэгте және т.б) меншіктеледі. әрбір іздеу механизмі салмақ коэффициенттерін берудің өз алгоритмдері бар – бұл әртүрлі іздеу машиналарының бір кілттік сөз арқылы сұрауға әртүрлі қорлар тізімін берудің бір себебі. Парақтар әрдайым жаңартылып отыратындықтан, онда индекстеу үрдісі де жиі орындалып отырылуы керек. Робот-өрмекшілер сілтемелерді аралай жүріп, индекстен тұратын файлды құрады, ол үлкен болуы мүмкін. Оның көлемін азайту үшін ақпарат көлемін минимизациялау мен файлды сығуға жүгінеді. Өңделгеннен кейін мәліметтер үнемі жаңарып отыратын базада сақталады. Бірнеше роботтары бар іздеу машинасы секундына жүздеген парақтарды өңдей алады. Бүгінде мықты іздеу машиналары жүздеген миллион парақты сақтайды және күніне ондаған миллион сұранысты қабылдайды.

Индексті құруда көшірмелердің санын азайту тапсырмасы да шешіледі – қатесіз салыстыру үшін алдымен құжаттың кодировкасын анықтау қажеттігін ескерсек, тапсырма оңай емес. Бұдан да қиын тапсырмаға өте ұқсас құжаттарды айыру жатады (оларды «көшірме дерлік»

деп атайды), мысалы оларға мазмұны бір ал тақырыбы әртүрлі болып келеді. Бұл сияқты құжаттар Желіде өте көп – мысалы біреу рефератты көшіріп алып өз сайтында басқа атпен басып шығаруы мүмкін. Қазіргі заманғы іздеу машиналары барлық бұл проблемаларды шешуге мүмкіндік береді.

Индекс арқылы іздеу.

Индекс арқылы іздеу мынадан құралады, яғни пайдаланушы сұраныс құрастырып оны іздеу машинасына береді. Бірнеше кілттік сөздерді қолдануда сұраныс тілін пайдаланған пайдалы, оның негізін буль операторлары құрайды.

Ең жиі қолданылатын буль операторлары:

- AND – бұл арқылы біріктірілген барлық терминдер ұсынылған құжатта қатысуы керек. Кейбір іздеу жүйелері «+» белгісін «AND» орнына қолданады;

- OR – кем дегенде бір кілттік сөз «OR »-мен қатысты, ізделінетін құжатта болуы керек;

- NOT- «NOT»-тан кейінгі кілттік сөз ізделінетін құжатта кездеспеуі керек. Кейбір іздеу жүйелері «-» белгісін «NOT» орнына пайдаланады;

- FOLLOWED BY – кілттік сөздер бірінен кейін бірі кезектесіп келуі керек;

- NEAR – сөздердің бірі екінші сөзден белгілі санды сөздерден кейін келуі керек;

- тырнақшалар – тырнақша ішіндегі сөздер - бұл текст фрагменті құжат немесе файл ішінде кездесуі тиіс. Айта кетейік, сұраныс тілі семантикасы нақты бір іздеу машиналарында бір біріне ұқсамауы мүмкін, әдетте ол туралы іздеу машинасының нұсқауында мәлімет келтіріледі.

Шектерінде логикалық комбинация анықталатын мәтін *іздеу бірлігі* деп аталады. Бұл сөйлем, абзац не бүкіл құжат болуы мүмкін. Түрлі іздеу жүйелерінде әртүрлі іздеу бірліктері қолданылуы мүмкін. Сөйлем шегіндегі іздеу тек индексінде толық мекенжай (адрес) бар жүйелерде ғана болуы мүмкін.

Пайдаланушы іздеу жүйесіне сұраныс жібергеннен кейін, ол сұраныс синтаксисін өңдейді, кілттік сөздерді индекстегі сөздермен салыстырады. Содан кейін сұранысқа жауап беретін сайттар тізімі релеванттылығына қарай рангіленіп, пайдаланушыға берілетіндей іздеу нәтижесі құрастырылады.

Бақылау сұрақтары:

1) Интернетте қажетті ақпаратты іздеудің жалпы принциптері қандай?

2) Іздеу машинасының жұмыс механизмі қандай?

3) Интернетте ақпарат іздеу технологияларында индекс ұғымы нені білдіреді?

4) Индексті құру принциптері қандай?

8 Дәріс №8. Интернет сервистері. Электрондық пошта. E-mail сервисінің жұмыс істеу механизмі. E-mail-дің екі протоколы. Электрондық поштаның адресі

Дәрістің мақсаты: интернет сервистерінің жұмыс жасау механизмімен танысу.

Дәрістің мазмұны: екі сервис – екі протокол. Пошталық клиенттің негізгі функциялары. Хатты жіберу және жеткізу. Арнаулы таңбаларды және толтырма хабарламаларды жөнелту.

Электрондық почта кез келген құжатты – ол мейлі қызмет жайлы жалпы мәлімет бола ма немесе жай хабар түріндегі мәтін бола ма – бәрі бір олардың ақпараттық негізін бірдей түрде нық ұстап, нақты әрі сенімді түрде жеткізе алады.

Электрондық поштаны пайдалану кезінде компьютерде әртүрлі арнаулы программалар қолданылады және олардың қажеттілігіне қарай бірінен біріне жеңіл ауысып отыруға болады. Мұндай программалар мынадай жұмыс атқарады:

- алынған мәліметтерді талдау және жаңа мәліметер дайындау;
- байланыс торабымен жылдам мәлімет алмасу.

Кәдімгі почта тәрізді электрондық почта да бір абонент пен екінші абонент арасында мәлімет алмасу үшін қолданылады. Жіберілетін мәліметте екі адрес көрсетілуі тиіс: хатты жіберуші және оны алушының аты-жөні мен оның компьютерінің желідегі адресі көрсетіледі. Хат иесінің адресін компьютер автоматты түрде өзі толтырады. Бұған қоса электрондық почта адрестерінде мынадай мәліметтер жазуға болады:

- мәлімет тақырыбының қысқаша сипаттамасы;
- хаттың көшірмесі тағы қандай адрестерге жіберілуі тиіс.

Электрондық почта жұмысы барысында хаттың тақырыбына қоса оның жіберілген мерзімі, уақыты т.с.с. керекті мәліметтер тіркеліп қалады.

Көптеген желілер алғашқы ретте ғылыми, конструкторлық және оқу орындарын байланыстыратын жүйе ретінде жасалған болатын. Сондықтан ұжымдық пікір-талас жүргізуге арналған желі мүмкіндігі телеконференция деп аталып, ол белгілі бір салада ғана қолдануға негізделген еді. Бірақ кейінен желілер практикада кең пайдаланылып, оның алғашқы ғылыми семинар, конференцияға арналған мүмкіндігі біршама шетте қала бастады.

Телеконференция ұйымдастыру кәдімгі кітапхана немесе архив жұмысына ұқсас жүргізіледі. Мұнда да көпсатылы тақырыптық каталогтар мен олардағы мәліметтерді сақтау ісі ұйымдастырылады.

Бірсыпыра байланыс тораптарының файлдық серверлері өз абоненттеріне өздерінде жинақталған ақпараттық материалдарды, яғни

файлдар архивін пайдалануды ұйымдастырып жүр. Ол материалдар мәтіндік құжаттардан, кітаптардан, сызбалардан, компьютерлерге арналған программалардан т.б. тұрады. Бұл мәліметтер ұзақ уақыт сақталады және олардың көлемі де үлкен болады.

Интернетке кіру рұқсат етуді регистрациядан өткізу уақытында ISP қолданушыға пошталық жәшікке дискінің белгілі-бір көлемін, пошталық жәшіктің адресін (E-mail Account Address), қолданушының атын (E-mail Account Login Name) және поштаға заңсыз кірудің рұқсатынан арылу үшін парольді (E-mail Account Password) бөліп береді. Электрондық пошта адресі: қолданушының_аты@домен_аты форматында болады, мысалы, *auesis@aipet.kz*. «@» таңбасының сол жағындағы бөлік – бұл сервердегі пошталық жәшіктің аты (Account Name), мұнан бұл адресің иесі хаттардың алады (берілген мысалда Auesis). Ережедегідей, қолданушының аты пошталық жәшіктің атымен сәйкес келеді. «@» таңбасының оң жағындағы бөлік *домен* деп аталады және осы пошталық жәшіктің орналасқан жеріне көрсетеді. Электрондық поштаның адресін пайдаланушы жеткізудің ақырғы бекеті, яғни поштаны көріп жатқан компьютер болып саналмайтынын ескере кету жөн. Әр қолданушы бірнеше адресстерді әртүрлі пошталық серверлерде регистрациядан өткізе алады. Бүгінгі таңда электрондық поштаның қызметін ақысыз көрсететін жүздеген серверлер бар, сондықтан да кез келген Интернет қолданушы әлемнің әр бөліктерінде пошталық жәшіктерін емін-еркін регистрациялауы мүмкін. Сондықтан электрондық пошта адресін сіздің үйіңіздегі компьютердің адресі айқындамайды, ал Сіз пошта алатын сервердің адресі беріледі.

Белгілі бір қолданушыда екі адрес регистрацияланған деп ойлайық: *sasha@ny-server.com* және *sasha@almaty-server.ru*.

Ол әр жәшігінен өзінің компьютеріне хаттар алады, бірақ біреуін ол Нью-Йорктегі серверден, ал екіншісін – Алматыдағы серверден көшіреді. Осыған байланысты электрондық поштаның көрсеткіштік адресациясы жеткізу маршрутын адрес анықтайтыны туралы айтады.

Екі сервис – екі протокол.

Электрондық пошта клиент-серверлік архитектураның принципімен құрастырылған. Қолданушы клиенттік программамен араласады, ол программа өз қатарымен пошталық сервермен араласады. Поштаны жіберу және алу процедурасы әртүрлі дәрежеде жеке адамның анықталуын (идентификация личности) сұрайтыны айқын, осыдан мұнда кәдімгі поштадағыдай толық ұқсастық (аналогия) көрінеді: сізге өзіңіздің пошталық жәшіктің ішінен хатты алу үшін кілт керек. Бұл жағдайда кілт сіздің поштаны алу құқығы бар екендігін растайтын автоматизация құралы болып табылады. Хатты жіберу кезінде авторизация міндетті емес. Жіберу және алу әртүрлі дәрежеде жеке адамның анықталуын сұрайтынына байланысты екі түрлі – хатты жіберуге және алуға арналған протоколдар бар. Хатты жіберу кезінде авторизация міндетті еместігіне қарамастан, бүгінгі таңда

провайдерлердің көпшілігі қауіпсіздік және спаммен күресу ойымен оны енгізу жоғары қойылады.

Хаттарды жөнелту үшін SMTP протоколы (Simple Mail Transfer Protocol – поштаға сілтеме қарапайым протоколы) және оған сәйкес SMTP-серверлері қолданылады. Көбінесе поштаны жіберу сіздің пошталық серверіңіздің интернет-провайдерінде болады, бірақта бұл онша міндетті емес. Әдетте SMTP-серверлер идентификацияны талап етпейді, сондықтан сіз хатты басқа да осындай серверден жіберсеңіз де болады. Пошталық хабарламаны алу үшін қазірі уақытта тек нақты қолданушының поштасын серверден алып тұратын және сондықтан жәшікке кіруге рұқсат ететін құқықтық авторизацияны сұрайтын POP3 протоколы (Post Office Protocol – пошталық офис протоколы) көп қолданылады.

Пошталық клиенттің негізгі функциялары.

Барлық пошталық клиенттердің негізгі функциялары – хабарламаларды алу, оларды автономды режимде көруді ұйымдастыру, хабарламаларды сорттау, жауап хабарламаларын дайындауды автоматизациялау және адрестік кітапшаны қолдау.

Хатты жіберу және жеткізу.

Интернетке қосылғаннан кейін, клиенттік программа пошталық сервермен байланысып, оған жіберушінің пошталық адресін және хабарламаның мәтінінің өзін жібереді. Поштаны жіберу кезінде клиенттік программа шығыс поштаның серверімен, яғни SMTP-сервермен 25 нөмірлі портқа SMTP протоколы арқылы қосылып, ара қатынасқа түседі. Пошта жіберілетін SMTP-серверінің аты клиенттік пошталық программаға оны күйге келтіру кезінде алдын-ала енізілу керек. Осы процесті мұқият қарастырайық. Хат жіберушінің серверіне жеткізілгеннен кейін, жіберушінің SMTP-сервері алушының серверімен байланысу керек. Бұл үшін оған алушының SMTP-серверінің IP-адресін білу қажет. Осы адресті білу үшін, ол DNS-серверге алушының SMTP-серверінің IP-адресін білуге сұраныс тастайды.

Егер де қайсы-бір себеппен жіберушінің SMTP-сервері алушының SMTP-серверімен байланысқа түсе алмаса, онда жіберілім жеткізілу үшін кезекке тұрады. Әдетте әр 15 минута сайын кезектегі хатты қайта жөнелту әрекеті өндіріледі. Шамамен 4 сағаттан кейін жіберушіге проблема туралы хабарлама жіберіледі, ал 5 күн өткен соң серверлердің көпшілігі әрекеттерін тоқтатып, жіберушіге жіберілменген поштаны қайтарады, сондықтан хат із-түссіз жоғалып кете алмайды.

Егер пошталық клиент пен SMTP-сервердің қатынас протоколына қарасақ, оның жетерліктей қарапайым екендігіне көз жеткізуге болады. Мұнда интуитивті түсінікті командалар қолданылады: мысалы HELO (таныстырыламын), MAIL FROM (жіберушіні анықтаймын), RCPT TO (алушыны анықтаймын) және т.с.с.

Жіберушінің SMTP-сервері алушының SMTP-серверімен байланысқа түскен сәтте-ақ, ол жіберілімді жөнелтеді. Алушының сервері адресте

көрсетілген атты қолданушының бар екендігін анықтайды және оның жәшігіне жіберілім жөнелтеді.

Пошта серверде орналасқаннан кейін, алушы оны сол жерден көшіріп алуға мүмкіндік алады. Пошталық жәшіктен жиналған поштаны алу кезінде, клиенттік программа POP3-сервермен POP3 протоколы арқылы байланысады. Интернетке кірген кезде өзіңіздің пароль мен логинді көрсеткендіктен кейін, әдетте поштаны алу кезінде осы мәліметтерді қайта енгізу керек емес. Сіздің пошталық клиентіңіз POP3-сервермен байланысып, локальді машинаға электронық пошта жіберілімдерінің копияларының жөнелтуін анықтайтын бұйрықтарды жібереді.

Әдетте, пошта алынғаннан кейін пошталық клиентте керісінше көрсетілмесе, сервердегі хабарламалар өшіріледі. SMTP-сервер секілді, POP3-сервер алушының пошталық клиентпен «сөйлесу» кезінде интуитивті түсінікті командалар жиынтығын қолданады: USER (қолданушының ID енгізіңіз), PASS (пароль енгізіңіз), QUIT (POP3-серверден шығыңыз), DELE (хабарламаны өшіріңіз).

Егер SMTP-протокол қарапайым және тек қана серверге алушының адресі бар хаттардың мазмұнын жіберетін болса, онда POP3-сервермен жұмыс әлдеқайда күрделірек болатынын ескеру жөн, ол хаттарды бөлектеліп көшіруді іске асырады, үлкен хаттардан бас тартуға жол береді және т.б.

Поштаны қабылдау үшін пошталық серверден хаттарды таңдамалы түрде компьютерге көшіріп алуға, папкалармен жұмыс істеуге және т.б. мүмкіндік беретін әлдеқайда жаңартылған IMAP-протокол қолданылуы мүмкін.

Электрондық хат адресатқа жетпеген кезде, бірнеше себептермен болуы мүмкін. Мүмкін, алушының сервері берілген жіберушінен хаттар алмаған жағдайда. Мұнан басқа, егер сервер жұмысы аса көп болса және сұранысты қарастыралмаса, жіберілім кері қайтарылады. Егер хат алушы серверімен жоқталмаса да, ол қайта оралуы мүмкін, мысалы, алушы атын жазу кезінде қателессеңіз – жүйе мұндай атты алушының жоқтығы туралы хабарлайды. Және соңғысы, көрсетілген атты алушы бар болса да, оның пошталық жәшігі толып кеткен кездегі жағдай туындауы мүмкін.

Арнаулы таңбаларды және толтырма хабарламаларды жөнелту.

SMTP-протокол ASCII-дың барлық символдарын жіберуді рұқсат етпейді, ал олардың ішінен ағылшын алфавитіне сәйкес келетін және ASCII кодтаудың негізгі кестесімен айқындалады. ASCII кодтаудың екі кестесін анықтайтыны белгілі: базалық жетібиттік (0-127 нөмерлі символдар) және кеңейтілген сегізбиттік (128-255).

Кириллица символдары кодтаудың кеңейтілген кестесіне жатады, және SMTP-протоколы үшін олар арнаулы символдар болып келеді. Арнаулы символдарды жіберу кезінде әдетте MIME стандарты (Multipurpose Internet Mail Extensions – Интернеттің көпмақсаттың кеңейтілулерлі пошталық стандарты) қолданылады, ол арнаулы

символдарды жіберу және мәтіндік емес ақпаратты электрондық пошта арқылы жіберу үшін кодтауды рұқсат етеді, мысалы хатқа қосымшада орналастырылған графикалық файлдар.

Бастапқыда электрондық пошта файлдарды жіберу үшін арналмаған еді, сондықтан қайсыбір файлды жіберу үшін оның мәтіндік хабарламаға сәйкес қайта кодировка жасау керек. MIME стандарты *файлдың тақырыбы арқылы оның қандай типті мәлімет* (мәтін, графика, әуен және т.б.) *қамтитынын анықтай алады* және қосарланған файлдарды кодтаудың біртұтас әдісін ұсынады. MIME стандарттары қолданған кезде, кириллицаны кодтау проблемалары туындамайды.

Бақылау сұрақтары:

- 1) E-mail клиентін ISP регистрациясы қалай өткізіледі?
- 2) Электрондық поштаның жіберу және жеткізу механизмі қандай?
- 3) E-mail сервисінде қандай протоколдар қолданылады?
- 4) Арнаулы таңбаларды және толтырма хабарламаларды жөнелтудің ерекшеліктері?

9 Дәріс №9. Интернет сервисі. Файлдармен алмасу. FTP сервисінің жұмыс механизмі. FTP – клиенттер

Дәрістің мақсаты: FTP сервисінің жұмыс механизмі мен Интернет сервисімен танысу.

Дәрістің мазмұны: FTP файлдарын жіберу протоколы (FILE TRANSFER PROTOCOL). FTP-ресурсының адрес форматы.

FTP файлдарын жіберу протоколы(FILE TRANSFER PROTOCOL).

FTP (File Transfer Protocol – файлдарды жіберу протоколы) 1971 жылы ұйымдастырылды және қазіргі уақытқа дейін жақсы қолданылуда. FTP TCP/IP базалық деңгейіндегі протоколдарымен базаланады және өз алдына Интернетте компьютерлер арасындағы файлдар алмасуын көрсетеді.

FTP негізгі тағайындалуы – Интернеттегі файлдарды жойылған компьютерден локальдіге (Download) және локальді компьютерден жойылғанға (Upload) қайта жіберу (көшіру, қайта беру). FTP протоколының көмегімен сондай-ақ өз файлдарыңды жойылған компьютерден жоюға және атын өзгертуге болады. Айта кететін жайт, ақпаратты тек оқуға арналған WWW-серверлеріне қарағанда, FTP серверлері ақпаратты жүктеуге және де ақпаратты серверге енгізуді қамтамасыз етеді. Жекешеді, Web-беттерден конструкцияланатын файлдарды жіберу үшін, көбінесе FTP-протоколдары қолданылады. Әрине, серверде ақпаратты өзгерту қамтамасыз, тек осы ақпараттың иесіне берілуі қажет. FTP-серверіне қолданушының жолығуы

кезінде рұқсаты логинмен және парольмен жарияланады, бірақ ол үлкен дәрістерге арналған желіде сервер жоқ дегенді білдірмейді. Көптеген серверлерге уақытша атпен кіруге болады (мысалы, anonymous немесе guest) және бұл кезде сізге, тек оқуға арналған файлдардың шектеулі жиынтығы беріле алады.

FTP-ресурсының адрес форматы.

Жалпы жағдайда FTP-ресурсының URL форматы мынадай түрге ие: ftp://<user>:<password>@<host>:<port>/<url-path>,

мұнда:

- user – қолданушы аты (логин);
- password - пароль;
- host – домендік ат немесе сервердің IP-адресі;
- url-path – файлға жол.

Әдетте портты көрсетпейді, бірақ бұл жағдайда 21-стандарты қолданылады.

Жалпы рұқсаты бар серверге жолығу кезінде, қолданушының аты ретінде anonymous қолданып, ал паролі ретінде - өзінің почталық адресін қолданамыз. URL-дағы анонимдік FTP үшін қысқартылған синтаксис қабылданған: ftp: //<host>/<url-path>, яғни аты жоқ болған кезде, автоматты түрде anonymous аты қолданылады.

FTP-клиенттері.

FTP қызметі клиент-сервер архитектурасына негізделген. Клиенттік компьютерде программалық-клиент жіберіледі, ол сервермен байланысады және жібереді немесе файлдарды қабылдайды. FTP-серверге рұқсат алу FTP-клиенттерінің әртүрлі класстарының көмегімен жүзеге асады, атап айтқанда:

- консольдік клиент – бұл *ftp.exe* программасы, ол Windows операциялық жүйесімен бірге беріледі,
- FTP-клиент, браузерге енгізілген (мысалы, Internet Explorer немесе Netscape Navigator);
- FTP-клиент, файлдық менеджерге енгізілген (FAR немесе Windows Commander);
- FTP-клиент, HTML – редакторға енгізілген (HomeSite, Dreamweaver немесе FrontPage);
- Негізделген программалар (мысалы, CuteFTP немесе WS FTP).

FTP.exe көмегімен рұқсат беру.

ftp.exe – бұл консольдік клиент, оның графикалық интерфейсі жоқ және өте ыңғайлы. Біз мұны «бұл қалай жұмыс істейді» деген сұраққа жауап беру үшін мысалға алдық.

ftp.exe жүктеуі интерактивті сеансты шақырады: программа сізге командалық жолды қамтамасыз етеді және сауалдарды күтіп отырады. Диалог жүргізу үшін оншақты командалар қолданылады, олардың кейбіреуі төменде көрсетілген:

- cd [жойылған_директория] - каталогты ауыстыру;
- mkdir [директории_аты] - каталогты жойылған машинада құру;
- get [жойылған_файл] [локальдік_файл] – жойылған файлдың көшірмесін сіздің компьютерге беру. Егер локальдік файл аты берілмесе, ол жойылған файлдың атымен сәйкес келеді;
- rget [жойылған_файл] [локальдік_файл] – жойылған файлды ары қарай енгізу, егер оның жарты бөлігі локальді машинада болса. Бұл команда көбінесе біріктірудің мүмкін болған бөлінулерінде үлкен файлдарды алу үшін пайдалы;
- put [локальдік_файл] [өшірілген_файл] – файлды өшірілген жүйеге жіберу. Егер өшірілген файлдың аты көрсетілмесе, онда ол локальдік жүйедегі атаумен сәйкес келеді;
- delete [жойылған_файл] - жойылған_файл атты файлды өшіру;
- close – жойылған сервермен FTP-сеансын бөлу және командалық интерпретаторға қайтару;
- bye — FTP-серверімен жұмысты аяқтау (интерпретатордан шығуды қамтамасыз етеді).

Командалардың толық тізімін және қосымша мәліметтерді сәйкестендірілген RFC-тен (RFC аббревиатурасы Request for Comments (түсіндіру ұсынысы) – Internet Engineering Task Force (IETF) организациясымен басылатын документтер сериясы және көптеген Интернетті және оның технологиясын қамтитын сұрақтарды қарастырады) алуға болады.

Ескерте кететін жайт, FTP-протоколы ұзақ уақытты интерактивті біріктіруді, диалог жүргізуді және байланыс сеансын тоқтату командасы берілмегенше, біріктіруді қамтамасыз етеді. FTP-протоколы екі типті файлды түсінеді – тексттік және екілік, мұнда барлық тексттік емес файлдар екілік түрінде қабылданады. FTP-біріктірілу арқылы жүретін жұмыс тексттік хабарламалардың ауысымы (қызметтік командалар) сияқты жүзеге асады, және де екі компьютер арасында ауысымда болатын файлдармен де жүзеге асады. Жұмыстың консольдік формасы қолданушылар үшін өте қолайлы емес, бірақ ол компьютер қай команданы орындап жатқанын түсінуге қолайлы жағдай береді.

Бақылау сұрақтары:

- 1) FTP-сервисінің Интернетте тағайындалуы қандай?
- 2) FTP-ресурсының Интернеттегі формат адресі қандай?
- 3) Қандай FTP-клиенттері Интернетте қолданылады?
- 4) Консольді FTP-клиенттерімен жұмыс кезінде қандай командалар қолданылады?

10 Дәріс №10. Интернеттегі мәліметтерді қорғау. Цифрлық қолтаңба. Криптография және Интернет. Симметриялық және

асимметриялық кілттер. Цифрлық қолтаңбаның механизмі. Қауіпсіздік проблемалары

Дәрістің мақсаты: интернеттегі мәліметтерді қорғау мен қауіпсіздік проблемаларын шешу жолдарымен таныстыру, криптография мен интернеттің байланысын түсіндіру.

Дәрістің мазмұны: симметриялық және асимметриялық кілттер. Цифрлық қолтаңбаның механизмі. Интернет желісіндегі мәліметтерді қорғау. Қауіпсіздік проблемаларын шешу.

Нақты мысал қарастырайық. Фирмасының директоры В фирмасының директорына өте қажетті бір құжатты электрондық почта арқылы жіберді делік. Қарап отырсақ мұнда қандай коммуникация қауіпсіздігі пайда болады. В фирмасының директоры бұл хатты алғаннан соң келесідей сұрақтар пайда болады. Шыныменде осы хатты А фирмасының директоры жіберді ма? (жіберуші идентификациясы). Бұл сұрақтың туындау себебі, бұл құжатты А фирмасының директоры ретінде басқа біреудің де жіберуі мүмкін. Бұл құжатты жіберу кезінде жолдан ұстап өзгертулер енгізген жоқ па? (жіберу аутентификациясы). Бұл құжатты қабылдаушыдан басқа адамдар оқыған жоқ па? (құпияның сақталуы). Бәрімізге белгілі құпияны сақтау үшін мәліметтерді шифрлау арқылы жетуге болады. (жіберу конфиденциалы). Берілген 3 мақсаттарды шифрлау базасы арқылы шешуге болады, онымен криптография айналысады.

Криптография – (грекшеден аударылғанда Cryptos – құпия деген мағынаны береді) – бұл ғылым және шифрлау технологиясы мәліметтерді өзгертуге және авторлық құқықты сақтайды. Криптография тек қана тексттерді шифрланған формаға аударып қана қоймайды, сонымен қатар жүйеде жұмыс жасап отырған кезде қолданушының аутентификациясын және идентификациясының берілуін қадағалап отырады. Криптография ең басты қауіпсіз коммуникация болып табылады. Біз жүйеде жұмыс жасаған кезде тек қана адамдармен сөйлесіп қана қоймаймыз, сонымен қатар басқа да қызметтер барысында араласатынымыз бізге мәлім. Мысалға, біз қандай да бір серверден программа көшіретін болсақ, біз үшін осы сервер шығарушы – фирманың сервері ма, әлде біздің компьютерімізге вирус болып түсетін пираттық фирманың сервері емес па деген ойлар келеді. Жіберу кезінде құжатты жеке және публикалық кілттер арқылы шифрлауға болады, ал оның шифрын екі пардағы кілттер арқылы ашуға болады. Құжатты шифрлап, жеке кілт арқылы жіберсе, оның шифрын публикалық кілт арқылы ашуға болады, және де керісінше. Жеке кілт тек қана иесіне белгілі оны басқа біреуге беруге болмайды, осы уақытта публикалық кілт барлық корреспонденттерге ашық жария етіледі.

Қос кілттер – жеке және публикалық – оларды аутентификация және құпияны сақтау үшін қолдануға болады.

Екі адамның мәлімет алмасуы үшін екі қос кілт болуы қажет.

Шифрлау кезінде қос кілттің арқасында сізге публикалық кілтті корреспонденттерге жіберіп отыру қажет емес. Бұл кілтті жүйеге ашық жазып қою сізге ыңғайлы болады. Сол кезде барлық адамдар осы кілтті өздеріне жазып алып, сіздерге құпиялы мәліметтерді жібере алады.

Симметриялық және асимметриялық кілттер арқылы шифрлеу.

Әрбір уақытта ассиметриялық шифрлау симметриялық шифрлаудан тиімділігі жағынан жеңіліп қалады, сондықтан да көптеген адамдар шифрлау жүйесінде ассиметриялық және дәстүрлі симметриялық шифрлау жүйесін қолданады. Ашық кілтпен шифрлау симметриялық кілт қолданылады, бұл жіберілген мәліметті шифрлау үшін қолданылады.

Цифрлық қолтаңба.

Цифрлық қолтаңбаның механизмін түсіндіру үшін, бір жақты хэш функцияны енгізу қажет. Біржақты хэш функция бұл функция, шығарылған мәліметтің ұзындығын белгілі ұзындыққа айналдырады, оны жіберу дайджесті деп атайды. 16 байттық хэш функцияны шығару кезінде сіз 16 байттық мәлімдеме аламыз.

Хэштеу – бұл біржақты, т.б, шифрлауға қарағанда қайтарымсыз. Дайджест бойынша шығарылған мәлімдемені қайтаруға болмайды, бірақ оған идентификация жасауға болады. Нақты бір мысал қарастырайық. Мысалы А хэш функция арқылы дайджестті қандайда бір код ретінде алынды делік (код 1). Одан соң ол А өзінің жеке кілтін пайдаланып, сол документтің аналогының қолтаңбасы болатын дайджестті шифрлайды. Содан соң А ашық текстті және цифрлық қолтаңбалы В жібереді. В абоненті оны публикалық кілт арқылы шифрлап ашады да, бұл хаттың А келгеніне сенімді болады. Осылай аутентификация орындалады. Содан соң бұл хаттың жолда өзгертілмегені жөнінде тексеру қажет. Соңында В шифрлау арқылы дайджестті алады – код 1. Содан кейін А сияқты В –да хэш – функцияны пайдаланып, дайджестті қандайда бір код ретінде алады – код 2. Егер код1 және код 2 бір біріне сай келсе, сонда ғана В бұл тексттің жолда өзгертілмегеніне көзін жетізеді.

Осындай жағдайда, цифрлық қолтаңба және электрондық қолтаңба – бұл әдіс жіберушінің аутентификациясы немесе авторлық қолтаңба, бұл мәліметтің мазмұнының өзгертілмеуіне себеп. Цифрлық қолтаңба шифрлау арқылы қойылуы да мүмкін, сонымен қатар ашық жіберуде орындалуы мүмкін.

Электрондық ақпараттық ресурстар мен ақпараттық жүйелерді қорғаудың мақсаттары:

Электрондық ақпараттық ресурстар мен ақпараттық жүйелерді қорғау:

- электрондық ақпараттық ресурстардың тұтастығын және сақталуын қамтамасыз ету, оларды рұқсатсыз өзгертуге немесе жоюға жол бермеу;
- қол жетімділігі шектелген электрондық ақпараттық ресурстардың құпиялығын сақтау;

- электрондық ақпараттық ресурстарға қол жеткізу құқығын іске асыру;

- электрондық ақпараттық ресурстарды өңдеу және оларды беру құралдарына рұқсатсыз ықпал етуге жол бермеу мақсатында құқықтық ұйымдастырушылық және техникалық (бағдарламалық техникалық) шараларды қабылдауды білдіреді;

Электрондық ақпараттық ресурстар мен ақпараттық жүйелерді қорғау:

- электрондық ақпараттық ресурстарды құрсаулау, яғни ақпараттық жүйеге және ол ұсынатын электрондық ақпараттық ресурстарға қолжетімділікті шектеуге немесе жабуға әкелетін іс-қимылдар жасау;

- электрондық ақпараттық ресурстарды түрлендіру, яғни бағдарламаға, деректер қорына, материалдық жеткізушідегі мәтіндік ақпараттарға өзгерістер енгізу;

- электрондық ақпараттық ресурсты көшіру, яғни ақпаратты басқа материалдық жеткізушіге ауыстыру;

- құқық иесінің рұқсатынсыз бағдарламалық өнімдерді пайдалану;

Электрондық ақпараттық ресурстарды қорғауды ұйымдастыру.

Электрондық ақпараттық ресурстарды қорғауды:

- жалпыға бірдей қол жетімді электрондық ақпараттық ресурстарға қатысты - электрондық ақпараттық ресурстарды тарататын тұлға;

- қолжетімділігі заңмен шектелген электрондық ақпараттық ресурстары бар ақпараттық жүйенің меншік иесі, иеленушісі немесе ұлттық операторы;

- қолжетімділігін олардың меншік иесі немесе иеленушісі шектелген электрондық ақпараттық ресурстарға қатысты - электрондық ақпараттық ресурстардың меншік иесі немесе иеленушісі ұйымдастырады.

Криптография екі бөліктен тұрады: криптография және криптоанализ.

Криптография – бұл заңсыз қолданушылардан қорғау үшін ақпараттарды өңдейтін ғылым.

Криптоанализ – бұл дешифлеуді орындау және тәжірибеде оны қолдану әдістері туралы ғылым.

Криптографиялық терминдерде шығыс жолдауы ашық мәтінмен аталады. Шифрлеу дегеніміз шығыс мәтіннің мазмұнын басқалардан жасыру үшін өзгертуді айтады. Шифромәтін деп шифрленген хабарды айтады. Шифромәтіннен ашық мәтінді шығару процесін шифрден алып шығу дешифрлеу дейміз. Көбінесе шифрлеу және дешифрлеу процесінде кілт қолданылады, осы кілтті білген адам ғана шифрден мәтінді алып шығарады.

Шифрлеу алгоритм негіздері.

Криптоалгоритмге қарасты бірнеше классификация схемалары пайдаланылады. Барлық криптоалгоритмдердің классификациялар схемасының негіздері мыналар:

- құпиятізім. Жіберуші және қабылдаушы хабарламаны өздері ғана өңдей алады. Басқа адамдарға шифрлеу алгоритмі белгісіз болады;

- криптография кілтімен. Барлық адамдарға алгоритм белгілі, бірақ ол «кілтке» байланысты, ол кілт тек жіберуші мен қабылдаушыда ғана бар;

- симметриялық криптоалгоритмдер. Хабарламаны шифрлеу және дешифрлеу үшін кілт қолданылады;

- асимметриялық криптоалгоритмдер. Хабарламаны шифрлеу үшін «ашық» кілтті қолданады, ол барлығына белгілі, ал дешифрлеу үшін «жабық» кілтті қолданады, ол тек қабылдаушыға ғана белгілі.

Кез келген криптоалгоритм кілтімен біз құпиятізімге айналдыруымызға болады. Ол үшін бағдарламадағы қолданып жүрген кодты өзгерту керек. Қайта ашу мүмкін емес.

Алгоритмдер деректерге байланысты бөлінеді:

- орын алмастыру. Ақпараттар жиыны, байттар, биттер және т.б. өзгермейді, бірақ олардың қатар тәртібі өзгереді, сондықтан басқаларға ақпаратты қолдану мүмкін емес;

- ауыстыруды тексеру. Криптоалгоритм заңы бойынша ақпараттар жиыны өзгереді. Көбінесе бастапқы алгоритмдер осы топқа жатады.

Криптоалгоритмдер ақпарат жиынының көлеміне байланысты бөлінеді:

- ағындық шифрлер. Кодтау өлшем бірлігі бір бит болып табылады. Кодтау шешімі алғаш үздіксіз кіріске байланысты емес. Бұл сұлба ақпараттарды жіберу жүйесінде қолданады, яғни кейбір жағдайда ақпаратты жіберу кезінде ықтиярлы уақытта басталуы және аяқталуы мүмкін, не болмаса әлдеқалай тоқтап қалуы мүмкін. Көп қолданатын ағындық шифрлер – скремблерлер;

- блоктық шифрлер. Кодтау өлшем бірлігі бірнеше байттар тізбегі (қазіргі кезде 4-32) жатады. Кодтау шешімі осы блоктың барлық негізгі байттар түрінен тұрады. Бұл сұлба файлдарды кодтау және ақпараттар пакетін жіберу кезінде қолданады.

Кілт қолданатын алгоритмдер екі топқа бөлінеді:

- симметриялық алгоритмдер құпия кілтімен;

- асимметриялық алгоритмдер ашық кілтімен.

Айырмашылығы: симметриялық алгоритм шифрлеу және дешифрлеу үшін бір кілтті қолданады, ал асимметриялық алгоритм әртүрлі кілттерді қолданады. Дешифрлеу кілті мен шифрлеу кілті сәйкес келмейді.

Цифрлық қол қою.

Кейбір асимметриялық алгоритмдерді цифрлық қол қою генерациясында қолданады.

Цифрлық қол қою деп кейбір құпия кілтті қолданатын генерлирленген мәліметтер тізімін айтады. Цифрлық қол қоюды хабардың нақты жіберуші адамнан келгенін анықтау үшін пайдаланады. Құжатта цифрлық қол қою былай құрылады: құжаттан дайджесті (message digest) генерациялайды және

оған қоса ақпарат қосылады, құжатқа кім қол қойғаны, штамп уақыты, және т.б көрсетіледі. Шыққан қатар құпия кілтпен шифрленеді. Осы шифрленіп алынған бит цифрлық қол болып саналады.

Криптографиялық хэш-функциялар.

Криптографиялық хэш-функцияларды көбінесе дайджест хабарлау генерациясында цифрлық қол құру кезінде қолданылады. Хэш-функциялар хабарларды жазып алынған көлемді бірнеше хэш-мәндерге (hash value) бірдей етіп бөліп тастайды.

Кездейсоқ сандардың криптографиялық генераторлары.

Кездейсоқ сандардың криптографиялық генераторлары кездейсоқ сандардан құрайды және олар криптографиялық қосымшаларда қолданылады, мысалы – кілттерді генерациялау кезінде.

Шифрленген алгоритм.

Шешу жұмысы қиын болу үшін жақсы криптографиялық жүйелерді құрады. Оны іске асыру үшін көп күш жұмсау қажет емес, тек ұқыптылық пен базалық білім болу керек. Теориялық негізде алатын болсақ, барлық кілт мәндерін таңдап шығу әдісімен шифрленген алгоритмді кілтті қолдану көмегімен ашады. Егер кілт белгілі бір әдіспен тандалса, онда компьютердің керек қуаты экспоненциалды өседі, сәйкесінше кілттің ұзындығы да өседі.

Бақылау сұрақтары:

- 1) Интернетте мәліметті жіберу кезінде қандай мәліметті қорғау механизмі қолданылады?
- 2) Жіберуші идентификациясы, жіберу аутентификациясы, құпияны сақтау мәндері қандай?
- 3) Симметриялық және ассиметриялық шифрлеудің мәні қандай?
- 4) Цифрлық қолтаңба механизмінің алгоритмін түсіндір.

11 Дәріс №11. Интернетте пайдаланушыларды идентификациялау. Cookies механизмі. Cookies-ті қолдану. Cookies негізіндегі технологиялардың кемшіліктері.

Дәрістің мақсаты: Cookies механизмін қолдануды үйрету және механизмде орын алатын проблемаларды шешу жолдарымен танысу.

Дәрістің мазмұны: интернетте пайдаланушыларды идентификациялау. Cookies механизмі. Cookies-ті қолдану. Cookies негізіндегі технологиялардың кемшіліктері.

Cookies – кішкене мәтіндік жазбалар, олар пайдаланушының компьютерінде сервердің сұранысы бойынша браузермен сақталынады. Бұл мәтіндік ақпарат пайдаланушы компьютерінде жойылғанша сақталынады. Пайдаланушының web-серверге қатынасу тарихы сақталған cookies-ті көптеген серверлер жібереді. Бұл жағдай сайттарға қатынасушыларды нақты бақылай отырып, сайттарды пайдаланушыларға және олардың иелеріне қосымша сервистер ұсынуға мүмкіндік береді. Мысалы: сайт иелері өздерінің сайтың неше адам қарағанын, сайтқа бірінші болып кім кіргенін, кім қайталап кіргенін білу өте маңызды. Бұл мәселе *Cookies* технологиясының көмегімен оңай шешіледі.

Cookies технологиясын пайдалану пайдаланушыны есте сақтауға мүмкіндік береді, cookies файлдарынан оның атын, дербес келтірулерін және т.б. оқу арқылы cookies-тің уақыттық және тұрақты файлдарын ажыратады.

Cookies-тің жалпы санына (500 артық емес) және бір сервер үшін сақталған cookies-тердің максималды санына (20-ға жуық) шектеулер бар.

Cookies-тердің шамасы аз және мәліметтердің үлкен көлемін сыйғыза алмайды. Әдетте, осы немесе басқа келуші кірген сайттар, оған көрсетілген жарнамалар, ол тапсырыс берген тауарлар тізімі және т.б. туралы ақпараттар Web-серверде сақталынады, ал cookies осы ақпараттарды іздеу үшін пайдаланылады. *Cookies* технологиясы жекелеген дербес беттерді жасауға мүмкіндік береді. Мысалы: егер сіз өз cookies-ті қандай да ауа-райын көрсететін сайтқа тіркелу кезінде берсеңіз, онда ол арнайы сіздің аймағыңыз үшін ауа-райын хабарлап тұрады. Электронды коммерция сайттары cookies-ті сатып алушылар кәрзеңкесін жасау үшін қолданылады. Сіздің кәрзеңкеңізге қосып жатқан барлық өнімдер туралы ақпараттар Web-сервердің мәліметтер базасында сіздің ID-іңізбен бірге сақталады. Егер сіз шотыңызды алғыңыз келсе, серверге сіз тапсырыс берген барлық тауарлар мәлім, сондықтан оған мәліметтер базасынан олардың құны туралы мәліметтер алу және сізге шотты беру қиын емес. Басқа компьютерден Web-сайттарға кіру барысында олар компьютерге қажет емес cookies-терді енгізуі мүмкін (компьютер иесінің емес, яғни қонақтың келтірулерімен ассоциацияланады).

Осындай жағдайда cookies-ті орналастыруға тыйым салып немесе жұмыстың аяқталуымен оны жоюға болады.

Cookies-ті жою сіздің компьютеріңіздің жұмыс қабілеттілігі жағынан тиімді, бірақ есте сақтаған жөн, егер сіз жиі кіретін сайтқа тиісті cookies-ті жойсаңыз, онда бұл cookies-термен бірге сіздің келтірулеріңіз жойылуы мүмкін.

Cookies-те қандай проблемалар пайда болады?

Егер қандай да бір сайтқа бір ДК-ді пайдалана отырып бірнеше адам қатысса, онда келуші Web-сервер әртүрлі келушілерді бір адам ретінде қабылдайды және олардың дербес келтірулерін шатастырады.

Егер сіз интернетке кіру үшін әртүрлі компьютерді пайдалансаңыз (біреуі үйде, екіншісі офисте) онда әрбір жағдайда барлық 3 компьютерде әртүрлі cookies-файлдар болады. Сонымен қатар cookies-тер өшіріледі (мысалы: жүйені қайта орнату барысында). Сол себептен егер сіз cookies-ті жойсаңыз және алдында кірген сайтыңызға қатыссаңыз, ол сізді жаңа пайдаланушы ретінде қабылдайды.

Бұл қиыншылықтардың барлығын сайтта тіркелу арқылы айналып өтуге болады. Бұл жағдайда сервер сіздің қай компьютерден кіріп отырғаныңызға тәуелсіз сіздің логиніңізбен, парольмен бірге cookies сақталады және сізге дұрыс ақпарат ұсынылады. Cookies мәтіндік түрде сақталғандықтан, пайдаланушы оны жоя алады немесе өзгерістер енгізе алады, Web-қолданбаны құрастырушылар әдетте cookies-те тек маңызды мәліметтерді сақтамайды және Web-сервердің жұмысын ол пайдаланушы дискіне орналастыруға тыйым салған жағдайда да жұмыс жасайтындай етіп ұйымдастырады. Дискіде cookies-тің болуы пайдаланушы қандай сайттарға кіргенін талдауға, кейбір жағдайда пайдаланушы нақты сайтқа хабарлаған мәліметтерді де талдауға мүмкіндік береді.

Cookie көмегімен қандай жұмыстар атқаруға болады?
Cookies өздерінше ешқандай жұмыс атқара алмайды, бұл тек қана мәтіндік ақпарат. Дегенмен, сервер cookies ақпаратын оқиды, сол ақпаратты сараптау негізінде басқа да әрекеттерді орындайды. Мысалы, авторизациялық қатынас кезінде WWW арқылы cookies-те сессия кезіндегі login және password қолданушыға әрбір документке сұраныс кезінде енгізе бермеуге мүмкіндік береді, ол парольмен қорғалады.

Интернеттегі жарнамалық бизнесте cookie механизмі кең қолданылады.

Cookie форматы мен синтаксисі.

Cookie HTTP бастапқы бетінің бір бөлігі. Өрістің толық сипаттамасы Set-Cookie HTTP бастапқы бет:

```
Set-Cookie: NAME=VALUE; expires=DATE; path=PATH; domain=DOMAIN_NAME; se
```

NAME=VALUE – үтір, бос орынды, жолдарды көшіруді болдырмайтын символдардың жолы. NAME-cookie аты, VALUE - мәні. Қос нүкте, үтір, бос орын қолдануға болмайды.

Cookie өрісі үшін HTTP бастапқы беттің синтаксисі.
HTTP серверден құжат сұралған жағдайда, браузер өзінің cookie дің сервердің доменіне және басқа да ақпаратқа сәйкес болуын тексереді. Егер барлық шарттарды қанағаттандыратын cookie мәні табылатын болса, браузер серверге аты және мәні түрінде жібереді:

```
Cookie: NAME1=OPAQUE_STRING1; NAME2=OPAQUE_STRING2 ...
```

Бірауқытта cookie-ге бірнеше мән беруге болады. Егер, cookie өз браузерінде болатын NAME, domain және path параметрлерімен сәйкес келетін болса, жаңа мәнді қабылдаған болса, онда ескі мәні жаңаға ауысады. Басқа жағдайларда cookie жаңа мәндері ескі мәндеріне қосылады.

Құжаттарды кәштеу кезінде, мысалы, проху-сервермен, HTTP бастапқы беттің Set-cookie өрісі ешқашан кәштелмейді.

Егер проху-сервер жауапты қабылдайтын болса, ол жауап бастапқы бетте Set-cookie өрісінде болады. Сәйкесінше, егер клиенттік сұраныс Cookie бастапқы бетінде болса, онда ол серверге міндетті түрде жетуі керек, тіпті катал түрде If-modified-since параметрі орнатылған болса да.

Бақылау сұрақтары:

- 1) Интернетте cookies терминінің мәні қандай?
- 2) Cookies-ті пайдалану арқылы қандай мәселелер шешіледі?
- 3) Cookies технологиясын пайдаланудың қандай ерекшеліктері бар?
- 4) Cookies-те жұмыс жасау механизмі қандай?

АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІНІҢ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ
Ақпараттық жүйелер кафедрасы

БЕКІТЕМІН
ОӘЖ проректоры
С.В. Коньшин
« _____ » _____ 2016 ж

WEB-ТЕХНОЛОГИЯЛАР

5B070300 - Ақпараттық жүйелер, 5B060200 – Информатика
мамандықтарының студенттеріне арналған

КЕЛІСІЛДІ
ОӘБ бастығы
_____ М.А. Мустафин
« _____ » _____ 2016 ж.

АЖ кафедрасының _____ жылғы
отырысында қарастырылып, мақұлданды,
хаттама № ____.
Келісілді
АЖ кафедрасының меңгерушісі
_____ Ш.И. Иманғалиев

ОӘКБ төрағасы
_____ Б.К. Курпенов
« _____ » _____ 2016 ж

Құрастырушылар:
_____ Ш.И.Иманғалиев
_____ Н.А.Дауренбаева

Стандарттау маманы

« _____ » _____ 2016 ж.

Редактор

« _____ » _____ 2016 ж.

Шнар Ихсанович Имангалиев
Нуркамиля Алдангаровна Дауренбаева

WEB-ТЕХНОЛОГИЯЛАР

5B070300 - Ақпараттық жүйелер, 5B060200 – Информатика
мамандықтарының студенттеріне арналған дәрістер жинағы

Редактор Қ.С.Телғожаева
Стандарттау бойынша маман Н.Қ. Молдабекова

Басуға _____ қол қойылды
Таралымы 30 дана.
Көлемі 2,8 есептік-баспа табак

Пішімі 60x84 1/16
Баспаханалық қағаз №1
Тапсырыс _____ Бағасы 1440

«Алматы энергетика және байланыс университеті»
коммерциялық емес акционерлік қоғамының
көшірмелі-көбейткіш бюросы
050013, Алматы, Байтұрсынұлы көшесі, 126