

№7 дәріс. ДЕРЕКТЕРДІ САҚТАУ ЖҮЙЕЛЕРІ

Жоспары:

1. Деректерді сақтау жүйелеріне кіріспе
2. Деректерді сақтау жүйелерінің түрлері
3. Деректерді сақтау жүйелерінің архитектурасы
4. Заманауи технологиялар мен тенденциялар
5. Деректердің сақтық көшірмесін жасау және қалпына келтіру
6. Деректерді сақтау жүйелерінің мәселелері мен қоңыраулары
7. Қорытынды

Деректерді сақтау жүйелеріне кіріспе

Деректерді сақтау жүйелері (*АИТ*) қазіргі заманғы ұйымдардың ақпараттық инфрақұрылымының ажырамас бөлігі болып табылады, өйткені олар деректерді сақтауды, өңдеуді және қорғауды қамтамасыз етеді. Цифрлық технологиялардың дамуынан туындаған ақпарат көлемінің қарқынды өсуі жағдайында сенімді және тиімді сақтау жүйесін құру бизнестің табысты жұмыс істеуі үшін өте маңызды болады. Деректерді сақтау жүйелері ұйымдарға ақпаратты сақтауға ғана емес, сонымен қатар деректердің қол жетімділігі мен тұтастығын қамтамасыз ете отырып басқаруға мүмкіндік береді.

АШҚ-ның негізгі міндеттерінің бірі-құрылымдық (мысалы, мәліметтер базасы) және құрылымдалмаған (мысалы, құжаттар, суреттер және бейнелер) қоса алғанда, әртүрлі деректер түрлерін сақтауды ұйымдастыру. Бұл ақпараттың ұлғаюымен тиімді күресу үшін сақтау жүйелерінен жоғары икемділік пен масштабталуды талап етеді.

Деректерді тиімді басқару ұйымдардың өнімділігіне, олардың негізделген шешім қабылдау қабілетіне және тұтынушыларға жоғары сапалы қызмет көрсетуге тікелей әсер ететінін атап өткен жөн.

Деректерді сақтау жүйелерін сақтық көшірме жасау, мұрағаттау, деректерді ортақ пайдалану және аналитикалық процестерді қолдау сияқты әртүрлі мақсаттарда пайдалануға болады. Олар GDPR және HIPAA сияқты ақпаратты қорғау саласындағы нормалар мен стандарттарды сақтауды қоса алғанда, деректерді басқару стратегияларын жүзеге асыруда шешуші рөл атқарады. Қауіпсіздік пен құпиялылық мәселелеріне көбірек көңіл бөлу жағдайында ұйымдар ақпараттың ағып кету және жоғалу қаупін азайту үшін сақтау жүйелерін Мұқият таңдауы керек.

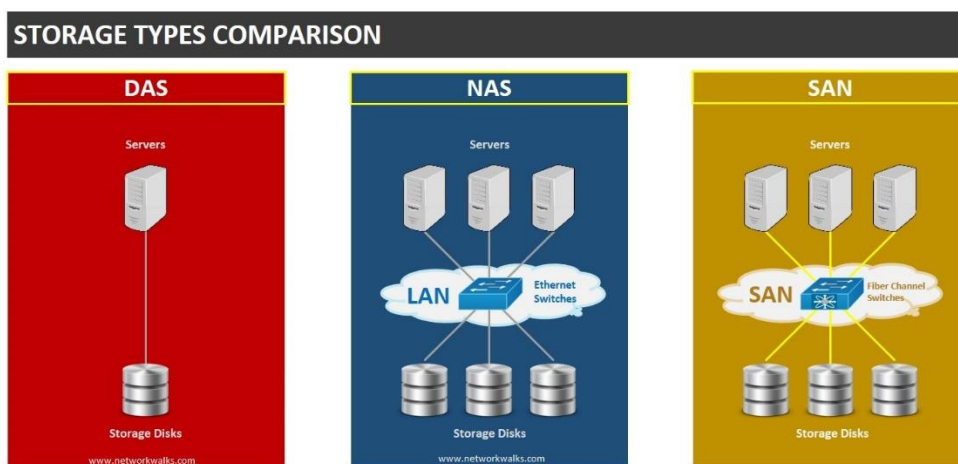
Сондай-ақ, АИТ инновациялар мен цифрлық трансформацияны қолдаудың маңызды элементіне айналатынын атап өткен жөн. Заманауи шешімдер сақтау жүйелерін бұлттық технологиялармен біріктіруге мүмкіндік береді, бұл әлемнің кез келген нүктесінен деректерге қол жеткізуге мүмкіндік береді және бизнеске нарықтың өзгеруіне тез бейімделуге мүмкіндік береді. Нәтижесінде деректерді сақтау жүйесін дұрыс таңдау және енгізу ұйымдардың табысты дамуына және

стратегиялық мақсаттарға жетуіне ықпал ететін бәсекелестік артықшылыққа айналуы мүмкін.

Деректерді сақтау жүйелерінің түрлері

Деректерді сақтау жүйелерінің бірнеше негізгі түрлері бар (Сурет 1), олардың әрқайсысының өзіндік ерекшеліктері бар және нақты мәселелерді шешуге арналған. Бұл түрлерді жергілікті, желілік және бұлтты сақтау жүйелеріне бөлуге болады. Жергілікті сақтау жүйелері-бұл компьютерлік жүйелерге немесе серверлерге тікелей Орнатылатын қатты дискілер (HDD) және SSD дискілері (SSD) сияқты құрылғылар.

Жергілікті SCHD деректерге қол жеткізудің жоғары жылдамдығын қамтамасыз етеді және операциялық жүйелерді, қолданбаларды және пайдаланушы деректерін сақтау үшін пайдаланылуы мүмкін. Дегенмен, олардың ауқымдылығы шектеулі және құрылғының физикалық зақымдалуына немесе жоғалуына байланысты тәуекелдерге ұшырауы мүмкін.



Сурет 1. Деректерді сақтаудың негізгі түрлері

Желілік сақтау жүйелері (NAS) жергілікті желідегі пайдаланушылар мен құрылғыларға Ортақ интерфейс арқылы деректерге қол жеткізуге мүмкіндік беретін икемді шешімді ұсынады. NAS шағын және орта бизнес үшін ыңғайлы нұсқа болып табылады, өйткені ол деректерді орталықтандырылған сақтау мен басқаруды қамтамасыз етеді. Мұндай жүйелерде әдетте сақтық көшірме жасау және деректерді қорғау функциялары бар, бұл ақпараттың қауіпсіздігін арттырады.

Желіге қосылған сақтау жүйелері (SAN) серверлер мен сақтау жүйелерін қосу үшін жоғары жылдамдықты желілерді пайдаланатын күрделі шешімдер болып табылады. SAN қол жетімділігі мен өнімділігі жоғары ірі ұйымдар үшін масштабталатын және жоғары өнімді сақтауды ұйымдастыруға мүмкіндік береді. Бұл жүйелер көбінесе деректер орталықтарында және мәліметтер базасы мен виртуалдандырылған орта сияқты үлкен көлемдегі ақпаратты сақтау үшін қолданылады.

Бұлтты сақтау жүйелері қазіргі заманғы ұйымдарда танымал бола бастады, өйткені олар икемділік пен масштабталуды ұсынады. Пайдаланушылар бұлтта

деректерді сақтай алады және оларға интернет арқылы әлемнің кез келген нүктесінен қол жеткізе алады. Amazon S3 және Google Cloud Storage сияқты бұлттық қызметтер жабдықтың жоғары бастапқы шығындарын болдырмайды және бизнес қажеттіліктеріне байланысты сақтауды жылдам масштабтау мүмкіндігін береді.

Сақтау жүйесінің әр түрінің өзіндік артықшылықтары мен кемшіліктері бар және дұрыс шешімді таңдау ұйымның нақты міндеттері мен талаптарына байланысты. Ең тиімді тәсілдер оңтайлы өнімділік пен сенімділікке қол жеткізу үшін әртүрлі типтегі жүйелерді біріктіруді қамтиды.

Деректерді сақтау жүйелерінің архитектурасы

Деректерді сақтау жүйелерінің архитектурасы деректерді тиімді басқаруға және қол жеткізуге мүмкіндік беретін компоненттердің құрылымы мен өзара әрекеттесуімен анықталады. Сақтау жүйесінің архитектурасын дұрыс таңдау ақпаратты сақтаудың өнімділігін, қауіпсіздігін және сенімділігін едәуір арттыра алады. Деректерді сақтау жүйелерінің негізгі архитектураларына модульдік, нысандық, блоктық және файлдық архитектура кіреді (Сурет 2).

Модульдік архитектура деректерді сақтау қажеттілігі артқан сайын жаңа модульдерді немесе құрылғыларды қосуға мүмкіндік беретін икемді шешім болып табылады. Бұл архитектура жеңіл масштабтауды қолдайды, бұл оны болашақта деректер көлемінің ұлғаюын күтетін ұйымдар үшін өте қолайлы етеді. Модульдік жүйелер қолданыстағы инфрақұрылымдармен оңай біріктіріліп, жаңарту шығындарын азайтады.

Нысан архитектурасы (мысалы, Amazon S3) суреттер, бейнелер және сақтық көшірмелер сияқты құрылымдалмаған деректерді сақтау үшін танымал бола бастады. Нысан жүйелерінде деректер бірегей идентификаторлары бар нысандар ретінде сақталады, бұл үлкен көлемдегі ақпаратты оңай басқаруға және оларға жылдам қол жеткізуге мүмкіндік береді. Нысан архитектурасы сонымен қатар деректердің сақтық көшірмесін жасау және қалпына келтіру процестерін жеңілдетеді, өйткені деректерді әртүрлі бұлттық орталар арасында оңай көшіруге және жылжытуға болады.

Блок архитектурасы деректерді жоғары өнімділік пен сенімділікті қамтамасыз ететін бекітілген өлшемді блоктарға бөледі. Бұл архитектура өнімділігі жоғары қолданбаларда және виртуалдандырылған орталарда қолданылады, өйткені ол ресурстарды тиімді бөлуге және деректерге қол жеткізу кідірістерін азайтуға мүмкіндік береді. Блокты сақтау жүйелері деректерді өңдеудің жоғары жылдамдығы мен сенімділігі өте маңызды ірі ұйымдар үшін өте қолайлы.

Файл архитектурасы деректерді файлдар мен қалталардың иерархиялық құрылымында сақтайды. Бұл деректер көлемі маңызды емес шағын ұйымдар үшін қолайлы шешім. Файлдық жүйелер деректерге ыңғайлы қол жетімділікті және басқарудың қарапайымдылығын қамтамасыз етеді, бірақ үлкен көлемдегі ақпаратпен жұмыс істегенде тиімділігі төмен болуы мүмкін.



Сурет 2. Блок, файл және объект архитектурасы

Сақтау жүйесінің архитектурасын дұрыс таңдау өнімділік, қол жетімділік, сенімділік және шығындарды қоса алғанда, бизнес талаптарына байланысты. Қазіргі заманғы жүйелер көбінесе әртүрлі архитектураларды біріктіреді, бұл оңтайлы нәтижеге қол жеткізуге және бизнес талаптарын қанағаттандыруға мүмкіндік береді.

Заманауи технологиялар мен тенденциялар

Деректерді сақтау жүйесіндегі заманауи технологиялар мен тенденциялар тез дамып келеді, бұл ақпарат көлемінің өсуіне және тиімдірек және сенімді шешімдерге деген қажеттілікке байланысты. Негізгі тенденциялардың бірі- әлемнің кез келген нүктесінен деректердің икемділігін, ауқымдылығын және қолжетімділігін ұсынатын бұлттық технологияларды белсенді енгізу. Бұлттық қызметтер ұйымдарға аппараттық құралдардың күрделі шығындарын азайтуға мүмкіндік береді және бизнес өскен сайын жылдам масштабтау мүмкіндігін береді.

Тағы бір маңызды тенденция-есептеу және желілік ресурстарды сақтау жүйелерімен біртұтас шешімге біріктіретін гиперконвергентті инфрақұрылымдарды (HCI) дамыту. HCI инфрақұрылымды басқаруды жеңілдетеді, техникалық қызмет көрсету шығындарын азайтады және ауқымдылықтың жоғары деңгейін қамтамасыз етеді. Бұл шешім әсіресе өз шығындарын оңтайландыруға және жұмыс тиімділігін арттыруға ұмтылатын компаниялар үшін тартымды болады.

Flash және NVMe (Volatile Memory Express емес) негізіндегі сақтау технологиялары да танымал бола бастады. Олар дәстүрлі қатты дискілермен салыстырғанда деректерді оқу мен жазудың айтарлықтай жоғары жылдамдығын қамтамасыз етеді. Бұл әсіресе дерекқорлар мен виртуалдандыру жүйелері сияқты жоғары өнімділікті қажет ететін қолданбалар үшін өте маңызды. Flash дискілерін пайдалану өнімділікті жақсартуға және жауап беру уақытын азайтуға мүмкіндік береді, бұл өз кезегінде сақтау жүйелерінің жалпы тиімділігін арттырады.

Сонымен қатар, жасанды интеллект пен машиналық оқытуды дамыту деректерді басқару мен аналитиканы жақсартуға ықпал етеді. Деректерді сақтау жүйелері интеллектуалды бола бастайды және тенденциялар мен ауытқуларды

анықтау үшін деректерді автоматты түрде талдай алады. Бұл ұйымдарға өзгерістерге тез жауап беруге және деректерді талдау негізінде процестерді оңтайландыруға мүмкіндік береді.

Ақырында, деректер қауіпсіздігіне баса назар аудару киберқылмыскерлер тарапынан өсіп келе жатқан қауіптер жағдайында өзекті бола түсуде. Ұйымдар шифрлауды, көп факторлы аутентификацияны және тұрақты қауіпсіздік аудиттерін қоса алғанда, деректерді қорғаудың заманауи шешімдеріне инвестиция салуы керек. Бұл ағып кету қаупін азайтуға және құпия ақпаратты қорғауға көмектеседі.

Деректердің сақтық көшірмесін жасау және қалпына келтіру

Деректердің сақтық көшірмесін жасау және қалпына келтіру деректерді сақтау жүйелерін басқарудың негізгі компоненттері болып табылады. Бұл процестер ақпаратты аппараттық ақаулар, адам қателіктері, вирустық шабуылдар немесе табиғи апаттар сияқты әртүрлі факторлардың әсерінен болатын шығындардан қорғау үшін қажет. Сақтық көшірме жасау мен қалпына келтірудің тиімді стратегиясы деректерді қорғап қана қоймайды, сонымен қатар бизнес континуитетін қамтамасыз етеді, бұл ұйымдарға оқиғалардан кейін өз қызметін тез қалпына келтіруге мүмкіндік береді.

1. Сақтық көшірме жасау принциптері

Сақтық көшірме-бұл деректерді қорғау үшін олардың көшірмелерін жасау және түпнұсқалары жоғалған жағдайда сақтау процесі. Сақтық көшірме жасаудың бірнеше негізгі тәсілдері бар:

Толық сақтық көшірме: бұл барлық деректердің толық көшірмесін жасау. Бұл әдіс максималды қорғауды қамтамасыз еткенімен, оны орындау және сақтау үшін көп уақыт пен ресурстар қажет.

Қосымша сақтық көшірме: бұл жағдайда тек соңғы сақтық көшірмеден өзгертілген немесе жаңа деректер көшіріледі. Бұл әдіс уақыт пен кеңістікте тиімдірек, бірақ қалпына келтіру ұзағырақ уақыт алуы мүмкін, өйткені соңғы толық сақтық көшірмені және одан кейінгі барлық қосымша көшірмелерді дәйекті түрде қалпына келтіру қажет.

Дифференциалды сақтық көшірме: бұл жағдайда соңғы толық сақтық көшірмеден кейін жасалған барлық өзгерістер көшіріледі. Бұл әдіс қосымша сақтық көшірмеге қарағанда ұзағырақ уақыт алады, бірақ қалпына келтіру қосымша сақтық көшірмеге қарағанда жылдамырақ.

2. Сақтық көшірмелерді сақтау

Деректердің сақтық көшірмелерін сақтау үшін әртүрлі тәсілдер қолданылады:

Жергілікті сақтау: деректердің көшірмелері бастапқы деректермен бір жерде орналасқан қатты дискілер немесе магниттік таспалар сияқты физикалық тасымалдағыштарда сақталады. Бұл әдіс жылдам қалпына келтіруді қамтамасыз етеді, бірақ сақтау орны физикалық зақымданған жағдайда деректердің жоғалу қаупін арттырады.

Қашықтан сақтау: сақтық көшірмелерді басқа физикалық жерде немесе бұлттық платформаларда сақтауға болады. Бұл жергілікті оқиғаларға байланысты деректердің жоғалу қаупін азайтады, бірақ қашықтағы ресурстарға қол жеткізу жылдамдығына байланысты қалпына келтіру уақытын арттыруы мүмкін.

Гибридті шешімдер: жергілікті және қашықтан сақтаудың үйлесімі. Көбінесе қалпына келтіру жылдамдығы мен деректерді қорғау арасындағы оңтайлы тепе-теңдікке қол жеткізу үшін қолданылады.

3. Деректерді қалпына келтіру

Деректерді қалпына келтіру процесі сақтық көшірмелерді шығаруды және оларды жұмыс жүйелеріне қалпына келтіруді қамтиды. Бұл үзіліс уақытын азайту үшін жылдам және сенімді болуы керек маңызды кезең. Қалпына келтіру процесінің негізгі аспектілері:

Қалпына келтіру жоспары: ұйымда деректерді қалпына келтіруге қажетті қадамдарды сипаттайтын нақты жоспар болуы керек. Бұл қандай деректерді қалпына келтіру керектігін анықтауды және оларды қалпына келтіру тәртібін қамтиды.

Қалпына келтіру сынағы: қалпына келтіру процестерін жүйелі түрде тексеру процедуралардың жұмыс істейтініне және деректердің қажетті көлемде және уақытта қалпына келтірілетініне көз жеткізуге мүмкіндік береді. Бұл оқиғаларға дайын болу үшін маңызды.

Деректерге басымдық беру: деректерді қалпына келтіруге басымдық беру маңызды. Бизнеске әсерін азайту үшін ең алдымен маңызды деректерді қалпына келтіру керек.

4. Сақтық көшірме жасау және қалпына келтіру стратегиясы

Сақтық көшірме жасау және қалпына келтірудің тиімді стратегиясы мыналарды қамтиды:

Сақтық көшірмелерді үнемі жасау: деректердің маңыздылығы мен жүйелердің қол жетімділігіне сәйкес келетін сақтық көшірме кестесін анықтау. Мысалы, маңызды деректер күнделікті немесе одан да жиі сақтық көшірме жасауды қажет етуі мүмкін.

Тәуекелдерді талдау: ұйымның ықтимал қауіптері мен осалдықтарын бағалау сақтық көшірме жасау мен қалпына келтірудің басымдықтарын анықтауға көмектеседі.

Қызметкерлерді оқыту: қызметкерлерді деректердің сақтық көшірмесін жасау және қалпына келтіру әдістеріне үйрету олардың оқиғалар болған жағдайда әрекет етуге дайын болуын қамтамасыз етеді.

Деректерді сақтау жүйелерінің мәселелері мен қоңыраулары

Сақтау жүйесіндегі көптеген жетістіктерге қарамастан, ұйымдар олардың тиімділігі мен қауіпсіздігіне теріс әсер етуі мүмкін бірқатар қиындықтар мен қиындықтарға тап болады. Негізгі мәселелердің бірі-өсіп келе жатқан деректер көлемін басқару. Ақпарат көлемі ұлғайған сайын ұйымдар оның қауіпсіздігін,

қол жетімділігі мен тұтастығын қамтамасыз етуде қиындықтарға тап болады. Деректердің сақтық көшірмесін жасау және мұрағаттау қажеттілігі барған сайын өзекті болып келеді, бұл айтарлықтай ресурстар мен уақытты қажет етеді.

Тағы бір маңызды мәселе-деректердің қауіпсіздігі. Кибершабуылдар мен ақпараттардың көбеюі жағдайында ұйымдар өз деректерін қорғау үшін шаралар қабылдауы керек. Бұл деректерді сақтау мен өңдеудің барлық деңгейлерінде қорғауды қамтамасыз ететін көп деңгейлі қауіпсіздік шешімдерін енгізуді қамтиды. Шифрлау және кіруді басқару сияқты заманауи технологияларға инвестициялау құпия ақпаратты қорғауды қамтамасыз ету үшін қажет болады.

Әр түрлі сақтау жүйелерін басқарудың күрделілігі көптеген ұйымдар үшін үлкен сынақ болып табылады. Көптеген компаниялар бірнеше сақтау жүйелерін пайдаланады, бұл тиімділіктің жеткіліксіздігіне және интеграцияның қиындауына әкеледі. Бұл басқару үшін айтарлықтай ресурстарды, сондай-ақ барлық жүйелердің дұрыс жұмыс істеуін қамтамасыз ету үшін білім мен дағдыларды қажет етеді.

Әртүрлі сақтау жүйелері арасындағы үйлесімділік пен деректерді тасымалдау да қиындық тудыруы мүмкін. Жаңа технологияларға немесе платформаларға көшу кезінде деректерді тасымалдау қажеттілігі туындауы мүмкін, бұл техникалық қиындықтар мен ақпараттың жоғалу қаупіне байланысты болуы мүмкін. Сондықтан ұйымдар деректерді тасымалдауды мұқият жоспарлап, үйлесімділік пен интеграцияның қарапайымдылығын қамтамасыз ететін шешімдерді таңдауы керек.

Деректерді сақтау жүйелерін сәтті басқару үшін ұйымдар осы қиындықтарды ескеретін стратегияларды әзірлеуі керек. Бұған заманауи технологияларға инвестициялар, қызметкерлерді оқыту және деректерді басқару жоспарларын әзірлеу кіреді. Деректерді сақтау жүйелерін тиімді басқару өнімділікті айтарлықтай жақсартады және ақпаратты сақтау шығындарын азайтады.

Қорытынды

Деректерді сақтау жүйелері қазіргі ұйымдардың ақпараттық инфрақұрылымының негізгі элементі болып табылады. Олар деректерді сенімді сақтауды, қол жетімділікті және қорғауды қамтамасыз етеді, бұл ақпарат көлемінің өсуі жағдайында маңызды бола бастайды. Деректерді сақтау жүйелерін дұрыс таңдау және енгізу бизнестің тиімділігін едәуір арттырады және операциялық шығындарды азайтады.

Деректерді сақтау жүйелерінің заманауи технологиялары мен архитектуралары ақпаратты басқарудың жаңа шешімдерін ұсына отырып, дамуын жалғастыруда. Бүлггі технологиялар, гиперконвергентті инфрақұрылымдар және Flash технологияларын пайдалану ұйымдарға өзгерістерге бейімделуге және нарықта бәсекеге қабілетті болуға мүмкіндік беретін жоғары өнімділік пен икемділікті қамтамасыз етеді.

Сонымен қатар, ұйымдар қауіпсіздікке, деректер көлемін басқаруға және әртүрлі сақтау жүйелерін біріктірудің күрделілігіне байланысты қиындықтарға дайын болуы керек. Сақтау жүйелерін басқарудың кешенді тәсілін қабылдау ұйымдарға осы қиындықтарды тиімді шешуге және бизнес мақсаттарына жетуге көмектеседі.

Деректерді сақтау жүйелері цифрландыру дәуірінде бизнестің табысты жұмыс істеуі үшін маңызды активке айналууда. Деректерді басқарудың дұрыс технологиялары мен стратегияларына инвестициялау өнімділік пен қауіпсіздіктің айтарлықтай жақсаруына әкелуі мүмкін, бұл сайып келгенде ұйымдардың табысты дамуына ықпал етеді.

Бақылау сұрақтары:

1. Ақпараттық қауіпсіздік инфрақұрылымы дегеніміз не, және оның негізгі компоненты қандай?
2. Ақпараттық қауіпсіздік инфрақұрылымындағы құпиялылық, тұтастық және қолжетімділік принциптерін (триадасы ЦРУ) түсіндіріңіз.
3. Киберқатерлердің негізгі түрлерін атаңыз және олардың әрқайсысының мысалдарын келтіріңіз.
4. Ақпараттық қауіпсіздік инфрақұрылымында брандмауэрлер (брандмауэры) қандай рөл атқарады?
5. Антивирустық бағдарламалық қамтамасыз етудің рөлі қандай және оның негізгі қызметтері қандай?
6. Криптография және шифрлау әдістері ақпараттық қауіпсіздікті қалай қамтамасыз етеді?
7. Аутентификация мен авторизация арасындағы айырмашылықты түсіндіріңіз.
8. Ақпараттық қауіпсіздік инфрақұрылымында қауіп-қатерлерді басқару және бағалау тәсілдерін сипаттаңыз.

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Бутузов, С. В. Системы хранения данных: проектирование и управление. М.: Издательство "Питер", 2020.
2. Parker, C. Data Storage Networking: How to Choose a Storage Area Network. New York: Wiley, 2021.
3. "Облачные технологии хранения данных." Москва: Издательство "Лаборатория знаний", 2022.
4. "Тенденции в области хранения данных: 2023 год." Журнал "ИТ-менеджмент", 2023.
5. "Архитектура систем хранения данных." Вестник информационных технологий, 2021.
6. "Современные технологии хранения данных." Рынок ИТ-услуг, 2022.

Қосымша әдебиеттер:

7. Amazon Web Services. Amazon S3 Documentation. Available online: <https://aws.amazon.com/s3/>.
8. IBM. IBM Cloud Object Storage. Available online: <https://www.ibm.com/cloud/cloud-object-storage>.
9. Gartner. Market Guide for Cloud Storage. Available online: <https://www.gartner.com/en/documents/3987505>.
10. NIST. NIST Special Publication 800-123: Guide to General Server Security. Available online: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-123.pdf>.