Ўзбекистон Республикаси Олий ва Ўрта махсус таълим вазирлиги

Наманган муҳандислик-педагогика институти

«Касб таълими» факултети

Касб таълими (Информатика ва АТ) кафедраси

«Ахборот хавфсизлиги» фанидан тажриба ишларни бажариш бўйича

УСЛУБИЙ КЎРСАТМА

Наманган – 2016 й

Ушбу услубий кўрсатма Касб таълими (Информатика ва ахборот теҳнологиялар) йўналиши бўйича таълим олаётган кундузги бўлим талабалари учун мўлжалланган бўлиб, “Ахборот хавфсизлиги” фанидан тажриба машғулотларини Ўтказиш бўйича барча йўриқномаларни ва тажриба иш вариантларини ўз ичига олган.

Услубий кўрсатмадан, “Ахборот хавфсизлиги” фанини мустақил ўрганувчи талабалар, магистрлар ва ўқитувчилар фойдаланишлари мумкин.

Муаллифлар: Ф. Ирисқулов Касб таълими (Информатика ва АТ) кафедраси ассистенти

Тақризчилар: С. Ҳошимов Касб таълими (Информатика ва АТ) кафедраси доценти

Услубий кўрсатма НамМПИ Касб таълими (Информатика ва ахборот теҳнологиялар) кафедрасининг умумий мажлисида кўриб чиқилган ва маъқулланган.
(Баённома №_____ «___» _____ 2016 йил)

Услубий кўрсатма НамМПИ «Касб таълими» факултети илмий-услубий кенгашида мухокама қилинган ва кўриб чиқиш учун институт илмий кенгашига тавсия етилган.
(Баённома №_____ «___» _____ 2016 йил)

Услубий кўрсатма НамМПИ илмий-услубий кенгашида мухокама қилинган ва чоп етишга тавсия етилган.
(Баённома №_____ «___» _____ 2016 йил)

1-2-Тажриба иши

Мавзу: Тизим ҳавфсизлиги. Маълумотларни ҳимоя қилувчи тизимлар. Тасодифий таъсирлар ва улардан маълумотларни ҳимоя қилиш усуллари

Ишнинг мақсади: Компютер хавфсизлигида заифликлар, Талабаларда қасддан қилинган таъсирлар хамда улардан ахборотни ҳимоялаш усуллари ҳақида қисқача назарий маълумотлар ва амалий кўникмалар ҳосил қилиш.

Масаланинг қўйилиши:

1) Компютер хавфсизлигида заифликлар.
2) Маълумотларни мухофаза қилишда кўзгули дисклардан фойдаланиш.
3) Кўзгули диск хосил қилишда RAID тизимлари хақида
4) Компьютер тармоқлари орқали маълумот узатишда компьютер протоколлари ва портлари хавфсизлиги (брандмауэр ёки FireWall тизимлари)
5) Берилган топшириқларни қўйилган вариантлар асосида бажариш.

Компютер хавфсизлигида заифлик (angl. vulnerability) термини тизимнинг кам ҳимояланган ёки очиқ жойини белгилашда ишлатилади. Заифлик дастурнинг хатоси ёки тизимни лойиҳалашда йўл қўйилган камчилик натижаси бўлиши мумкин. Заифлик ёки фақат назарий мавжуд бўлиши ёки машҳур експлойтга ега бўлиши мумкин. Заифлик кўп ҳолларда дастурчининг бепарволиги натижасидир, бироқ бошқа сабаблар ҳам бўлиши мумкин.

Бузғунчининг тажоввузини амалга оширишда фойдаланиши мумкин бўлган ахборот тизимининг ҳарқандай характеристикаси заифлик деб аталади. Бунда заифлик мақсадга мувофиқ ёки ўзи хоҳламаган ҳолда ишлатилаётганлигининг аҳамияти йўқ. Бузғунчи сифатида тармоқ ресурсларига хатолик бўлиб, билмаган ҳолда ёки ёмон ниятда ноқонуний рухсатга ега бўлишни амалга оширишга уринган корпаратив тармоқнинг ҳарқандай субъекти бўлиши мумкин.

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Ахборотни химоя килиш деганда:

- Ахборотнинг жисмоний бутунлигини таъминлаш, шу билан бирга ахборот элементларининг бузилиши, ёки йук килинишига йул куймаслик;
- Ахборотнинг бутунлигини саклаб колган холда, уни элементларини калбакилаштиришга (узгартиришга) йул куймаслик;
- Ахборотни тегишли хукукуларга эга булмаган шахслар ёки жараёнлар оркали тармокдан рухсат этилмаган холда олишга йул куймаслик;
- Эгаси томонидан берилаётган (сотилаётган) ахборот ва ресурслар факат томонлар уртасида келишилган шартномалар асосида кулланилишига ишониш кабилар тушунилади.

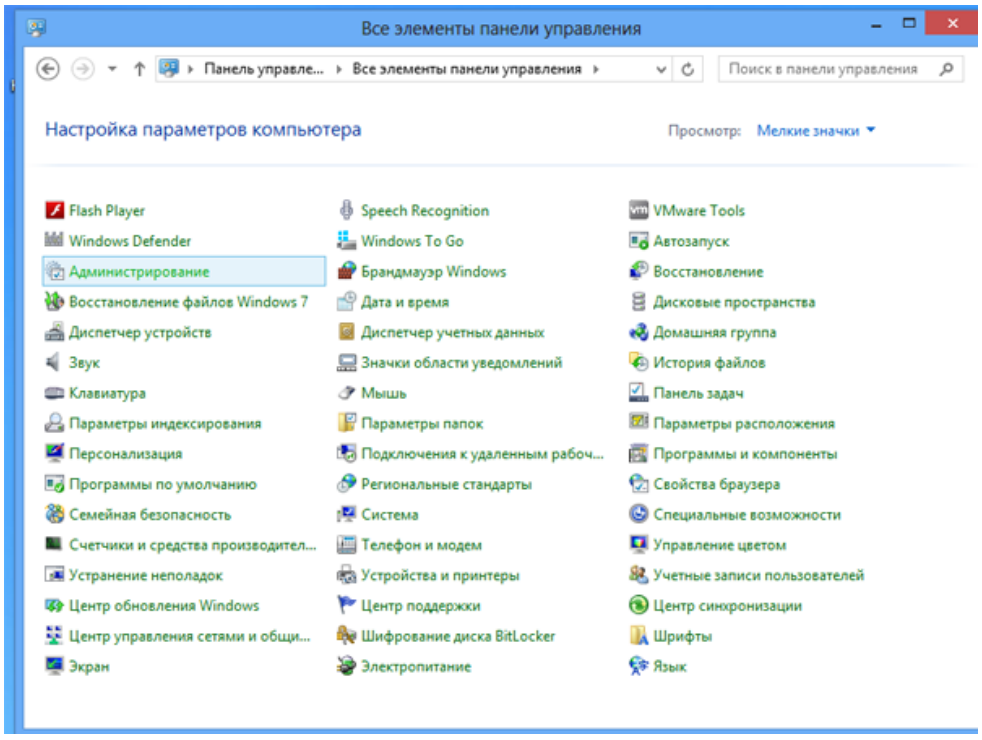
Тасодифий таъсирлар – бу системага талофот етказадиган ёки уни умуман ишдан чиқарадиган таъсирлар. Масалан, электр манбаининг бузилиши, қурилманинг ишдан чиқиши, ёнғин, сув босиши ва шу кабилар. Тасодифий таъсирлар натижасида информация бузилиши ёки йўқолиши мумкин. Шунинг учун қуйидаги информацияни ҳимоя қилиш ва тиклаш воситаларидан фойдаланиш мумкин:

Кўзгули дисклар (зеркальные диски) – булар дискларнинг физик зарарланиши билан боғлиқ йўқотишларнинг олдини олиш учун дискларни резервлаш мақсадида фойдаланиладиган дисклар.

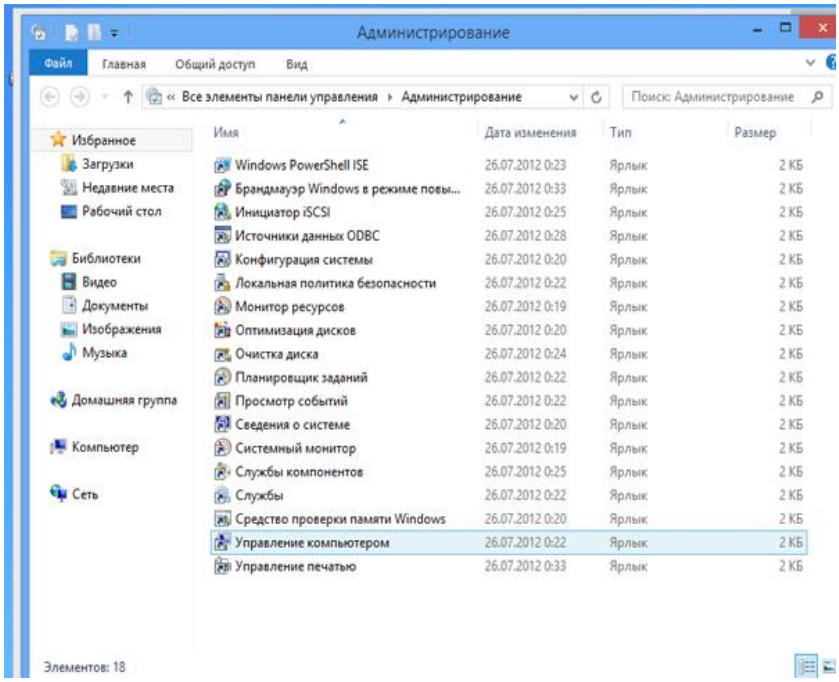
Дискларни резервлаш учун битта диск контроллерига 2 та мутлақо бир хил винчестер уланади ва операцион система шунга мувофиқ мослаштирилади. Сўнгра асосий дискдаги барча информация кўзгули диск деб номланувчи иккинчи дискда иккилантирилади.

Асосий диск зарарланганда махсус процедуралар ёрдамида кўзгули дискдан барча маълумотларни қайта тиклаш мумкин. қўшимча равишда диск йўлакчаларининг «қайноқ» резервлаш ҳам ишлатилади. Дискда «қайноқ» резервлаш соҳаси ажратиб олинади. Агар иш жараёнида дискда нуқсонли йўлакча топилса, бу йўлакча резервлаш соҳасидаги йўлакча билан алмаштирилади.

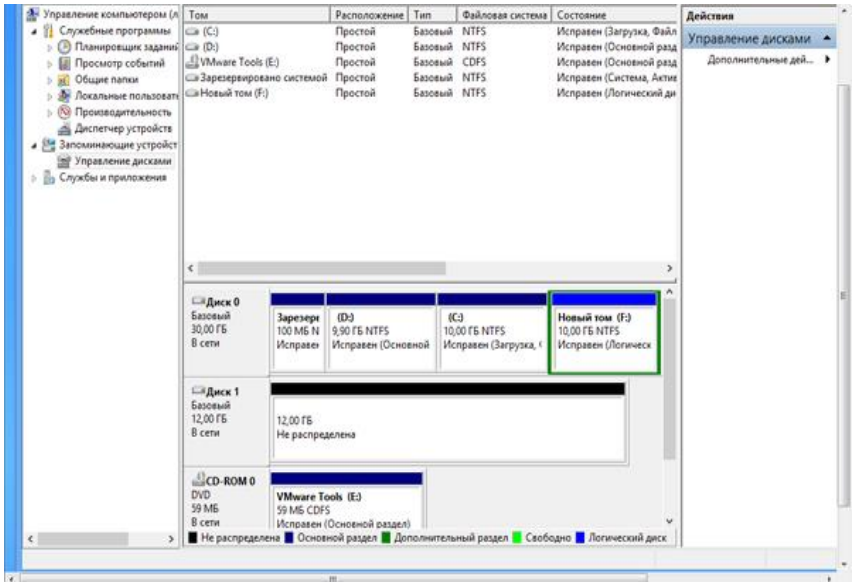
Кўзгули дискларни хосил қилиш учун, Панель управления кириб "Администрирование"ни танлаймиз.



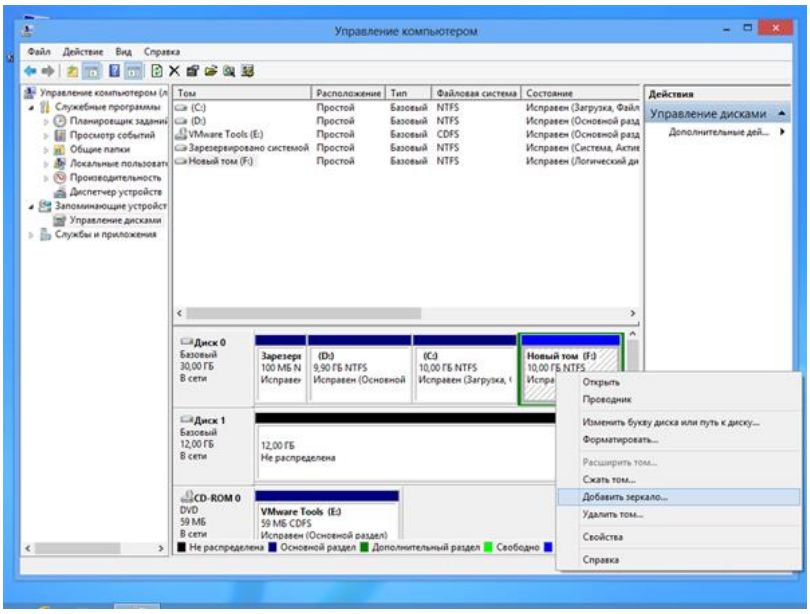
Администрациялаш бўлимидан "Управление компьютером"га ўтамиз



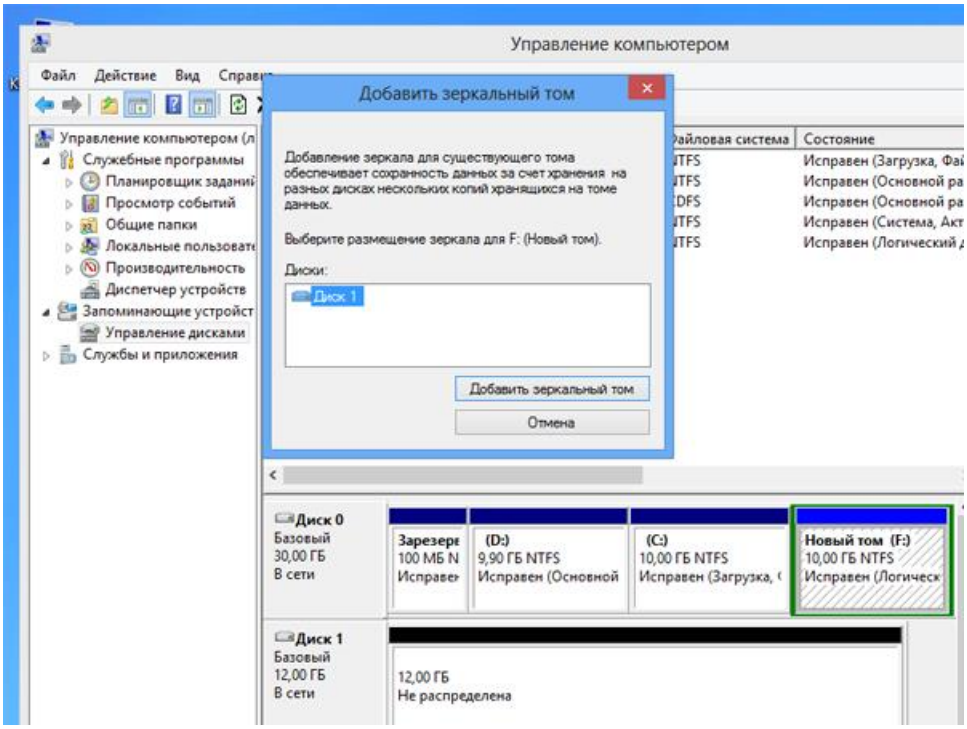
Управления компьютером ойнасидан "Управление дисками" бўлимига ўтамиз



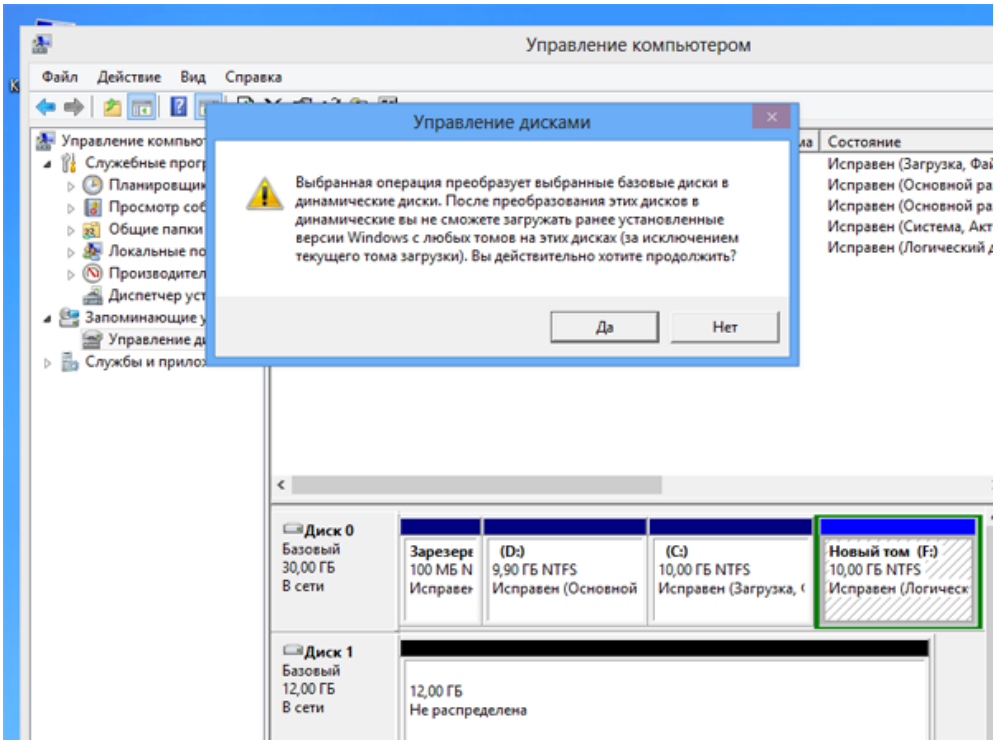
Контекс меню орқали керакли диск устида "Добавить зеркало" ни танлаймиз



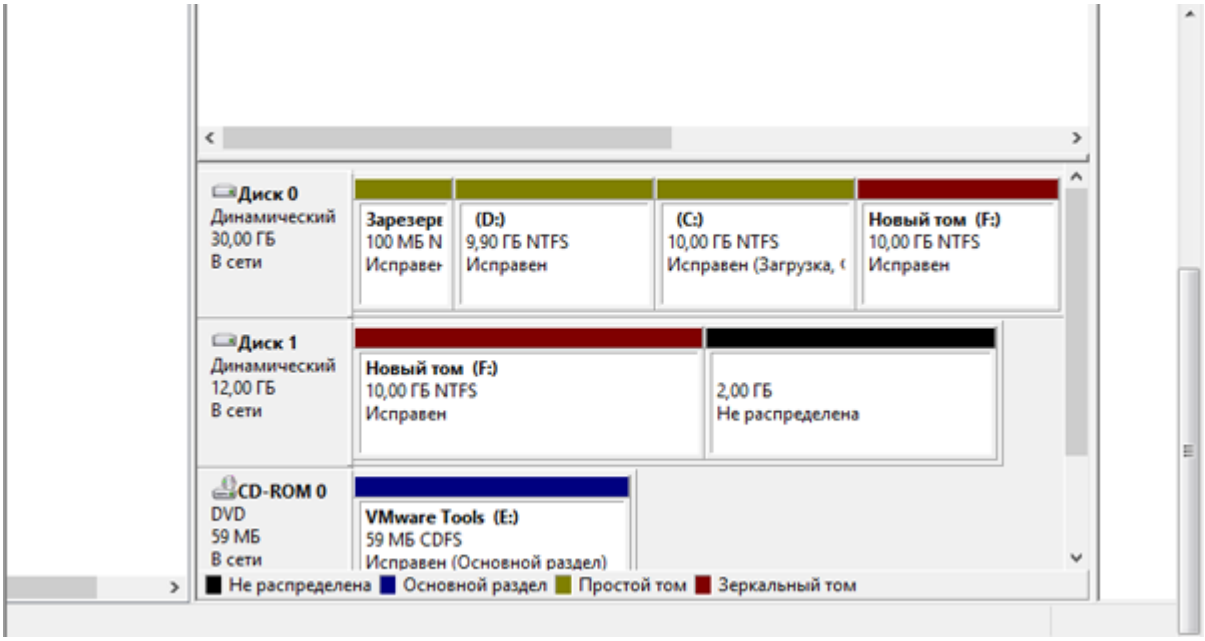
Тизим автоматик кўзгуни танлаш дискини сўрайди.



Керакли дискни рўйхатдан танлаб "Добавить зеркальный том" ёзуви устидан босамиз. Қуйидаги ёзув хосил бўлади.



Кўзгули диск хосил қилиш жараёни бошланади. F- даги барча маълумотлар кўзгули дискка нусхаси кўчирилади ва кўзгули диск динамик дискка айланади.



Хосил бўлган натижа.

Динамик диск қайта юкланишда фойдаланувчи учун кўринмас холатга келади.

RAID - Мустақил дисклар захира массиви

Дискли мссивнинг ишлаш қобилиятини юқори унумдорлиги.

“RAID 0” массиви

Барча RAID ларгақараганда RAID 0 енг кўп унумдорликка ега ва енг кам ҳимояланган. Дискларнинг сонига мутаносиб равишда маълумотлар блокларга бўлинади, бу еса юқори ўтказувчанликқобилиятига олиб келади. Мазкур тузилманинг юқори унумдорлиги паралелл ёзиш билан ва ортиқча нусха кўчиришлар йўқлиги билан таъминланади. Массив дискдаги харқандай дискнинг рад жавоби барча маълумотларни йўқотишга олиб келади. Бу босқич “striping” деб номланади.

Устунлиги:

- Катта маълумотларни киритиш – чиқаришда интенсив қайта ишлашни талаб қилаётган иловалар учун юқори иш унумдорлиги;
- қўллашда соддалиги;
- Ҳажм бирлиги учун пастқийматлиги.
- Камчилиги:
- Битта дискни ишдан чиқиши массивдаги қолган барча маълумотларни йўқолишга олиб келади.

“RAID 1” массиви

Массив дискиқурилмали ёки ойнали.

Duplexing 1 Mirroring

RAID 1 – mirroring – 2 та дискнинг ойнадаги акси. Ушбу массивнинг ортиқча тузилмалари уни юқори иш унумдорлиги билан таъминланади. Массив юқори таннархи ва иш унумдорлиги пастлиги билан ажралиб туради.

Устунлиги:

- Ишлатишда қулайлиги;
- Массивда нусха кўчирилаётганда қайта тиклаш оссонлиги;
- Иловаларда катта интенсив сўровлар учун етарлича юқори тез ҳаракатчанлиги.

Камчилиги:

- Бирлик ҳажмда 100% керагидан ортиқча қиммат;
- Маълумот узатиш тезлиги паст.

“RAID 2” массив

Массив дискини Хемминг коди билан ишлатиш.

Hamming Code ECC

RAID 2 – хатоликларни тузатиш учун Хемминг кодларини ишлатади. Кодлар бирламчи носозликларни ва иккиламчи носозликларни топишга имкон беради.

Устунлиги:

- Хатоликларни тезкор тузатишлиги;
- Катта ҳажмдаги маълумотларни юқори тезликда жўнацҳлиги;
- Дискларни кўпайтирилганга харажатлар камайганлиги;
- Ишлатишдақулайлиги.

Камчилиги:

- Дискларнинг камчилигида нархнинг баландлиги;
- Маълумотларни қайта ишлашда тўлиқлилигининг пастлиги.

“RAID 3” массиви

RAID 3 – дискларнинг бирида бошқарув маблағи билан байтлар босқичида маълумотлар “striping” асосида сақланади. Бу массив RAID 2 га ўхшаган ортиқча муаммоларга ега емас RAID 2 да ишлатиладиган маблағ бошқарув диски, хатолик билан ишлайдиган манбани топиш учун керак. Лекин кўпчилик замонавий текширувчи диск махсус товушлар билан рад жавоб берганини аниқлаш қобилиятига ега.

Устунлиги:

- Маълумотларни жуда юқори тезликда жўнатилганлиги;
- Дискни рад жавоб бериши массивнинг ишлаш тезлигига таъсир етмаганлиги ;
- Кам қопланган чиқимлар учун керагидан кўп амалга оширилганлиги.

Камчилиги:

- Кўллашда осон емас.
- Унга катта бўлмаган маълумотларниқайта ишлашда тезлиги паст.

Айнан кўзгули дискларни хосил қилишда RAID 1 қўлланилади.

Тармоқлараро экран — ҳимоялаш воситаси бўлиб, ишончли тармоқ, ва ишончсиз тармоқ орасида маълумотларга киришни бошқаришда қўлланилади.

Тармоқлараро экран кўп компонентли бўлиб, у интернетдан ташкилотнинг ахборот захираларини ҳимоялаш стратегияси саналади. Яъни ташкилот тармоғи ва интернет орасида қўриқлаш вазифасини бажаради.

Тармоқлараро экраннинг асосий функцияси — маълумотларга егалик қилишни марказлаштирилган бошқарувини таъминлашдан иборат.

Тармоқлараро экран қуйидаги ҳимояларни амалга оширади:

• ўринсиз трафиклар, яъни тармоқда узатиладиган хабарлар оқимини тақиқлаш;

• қабул қилинган трафикни ички тизимларга йўналтириш;

• ички тизимнинг заиф қисмларини яшириш билан Интернет томонидан уюштириладиган ҳужумлардан ҳимоялаш;

• барча трафикларни баёнлаштириш;

• ички маълумотларни, масалан тармоқ топологиясини, тизим номларини, тармоқ ускуналарини ва фойдаланувчиларнинг идентификаторларини Интернетдан яшириш;

• ишончли аутентификацияни таъминлаш.

Кўпгина адабиётларда **тармоқлараро экран** тушунчаси **брандмауер** ёки **Fire Wall** деб юритилган. Умуман буларнинг ҳаммаси ягона тушунчадир.

Тармоқлараро экран — бу тизим, умумий тармоқни икки қисмга ажратиб, тармоқлараро ҳимоя вазифасини ўтайди ва маълумотлар пакетининг чегарадан ўтиш шартларини амалга оширадиган коидалар тўплами ҳисобланади.

Одатда тармоқлараро экран ички тармоқларни глобал тармоқлардан, яъни Интернетдан ҳимоя қилади. Шуни айтиш керакки, тармоқлараро экран нафақат Интернетдан, балки корпоратив тармоқлардан ҳам ҳимоя қилиш қобилиятига егадир. Ҳар қандай тармоқлараро экран ички тармоқларни тўлиқ ҳимоя қила олади деб булмайди.

Brandmauer дан фойдаланганда асосан комьютерларда ишлатиладиган протоколь ва портлар химоясига ва уларни ишлашини назоратига урғу қаратилади.

Шундан келиб чиқиб қуйидаги протоколлар хақида маълумотларни билишимиз шарт.

HTTP - ing. *HyperText Transfer Protocol* — «гиппер матн юбориш протоколи»;

HTTPS (ing. *HyperText Transfer Protocol Secure*) — HTTP протоколини кенгайтирилган версияси бўлиб, маълумот шифрлаш усули орқали узатилади.

SMTP - ing. *Simple Mail Transfer Protocol* — почта юбориш оддий протоколи;

SMTP с SSL- почта юбориш шифрланган протоколи

SNMP - ing. *Simple Network Management Protocol* — тармоқ бошқариш оддий протоколи;

FTP - ing *File Transfer Protocol* — файллар юбориш протоколи;

TFTP (англ. *Trivial File Transfer Protocol*) - файллар юборишнинг оддий протоколи

TELNET – ing. TErminaL NETwork - матн интерфейсини тармоқ бўйлаб амалга оширишга ҳизмат қиладиган тармоқ протоколи;

SSH – ing. ***S****ecure* ***Sh****ell* — хафвсиз қобиқ;

SCP - ing. *secure copy* — файллардан нусха олиш RCP протоколи, SSH ни транспортида қўлланилади;

NFS – ing .*Network File System* — файл тизимига тармоқ руҳсатини берувчи протокол;

RTSP - *Real Time Streaming Protocol*, ҳақиқий вақт оқим протоколи;

BGP - ing. *Border Gateway Protocol*, чегара шлюзи протоколи.

XDR – ing. *External Data Representation* – маълумотларни ташқи кўриниши*;*

TLS - ing. *Transport Layer Security* — транспорт сатхини хавфсизлиги;

SSL - ing. *Secure Socket Layers* — ҳимояланган сокетлар сатхи;

PPTP – ing. *Point-to-Point Tunneling Protocol* — нуқта-нуқта туннел протоколи;

L2TP – ing. *Layer 2 Tunneling Protocol* — туннел иккичи даража протоколи;

TCP - ing. *Transmission Control Protocol* **–** маълумотлар алмашинуви, бошқарув протоколи;

UDP – ing. *User Datagram Protocol* — фойдаланувчилар датаграм протоколи; (*Datagram* – маълумотларни блоклаш);

SCTP – ing. *Stream Control Transmission Protocol* — бошқарилаётган оқим билан маълумотлар алмашинуви**.**

IEEE 802 – локал тармоқлар учун IEEE 802 стандарти;

ATM – ing. *Asynchronous Transfer Mode* — маълумотларни юборишнинг асинхрон усули;

DNS – ing. *Domain Name System* — домен номларининг тизими;

IMAP (инг. *Internet Message Access Protocol*) — электрон почтадан фойдаланишни амалий даражаси.

Топшириқ:

1. Кўзгули диск хосил қилишни ўрганиб чиқинг ва кўзгули дискдаги маълумотни қайта олиш усулини қўрсатинг.
2. Берилган вариант асосида WINDOWS операцион тизими химоялаш бошқарувларини (консоль) ўрганинг ва у хақда маълумот берувчи тақдимот яратиш.
3. Берилган вариант асосида WINDOWS операцион тизими протокол ва портларини ўрганинг ва у хақда маълумот берувчи тақдимот яратиш.
4. Шахсий протоколингизни яратинг.

№	Консол номланиши	Протокол ёки портлар номланиши
1.	Управление печатью	
2.	Локальная политика безопасности	
3.	Инициатор iSCSI	
4.	Windows PowerShell Modules	
5.	Брандмауэр Windows	
6.	Диспетчер служб IIS	
7.	Брандмауэр Windows в режиме повышенной безопасности	
8.	Локальная политика безопасности	
9.	Источники данных (ODBC)	
10.	Конфигурация системы(Msconfig)	
11.	Инициатор iSCSI	
12.	Планировщик заданий	
13.	Диспетчер служб IIS	
14.	Просмотр событий	
15.	Windows PowerShell Modules	
16.	Службы компонентов	
17.	Источники данных (ODBC)	
18.	Конфигурация системы(Msconfig)	
19.	Просмотр событий	
20.	Службы	
21.	Локальная политика безопасности	
22.	Конфигурация системы(Msconfig)	
23.	Средство проверки памяти Windows	

24.	Планировщик заданий	
25.	Управление компьютером	
26.	Системный монитор	
27.	Источники данных (ODBC)	
28.	Системный монитор	
29.	Диспетчер служб IIS	

Foydalanilgan adabiyotlar

1. William R. Cheswick and Steven M. Bellovin. Firewalls and Internet Security. Posted on March 24th, 2006
2. Matt Smith. “HackerProof: Your Guide To PC Security”. Posted on February 28th, 2011
3. Darmawan Salihun. “BIOS Disassembly Ninjutsu Uncovered”. Posted on October 1st, 2012
4. Ярочкин В.И. Информационная безопасность. Учебник для студентов ВУЗов М.: Фонд «Мир», 2003 – 640 б
5. G’aniev S. K., Karimov M. M., Tashev K. A. Axborot xavfsizligi/ O’quv qo’llanma. – T.: Aloqachi, 2008. – 423 b.
6. Костылов А.К. Информационное право: учебное право. Тюмень: Изд. Тюменск.гос.университет, 2004. 188 с.
7. Арипов М., Пудавченко Ю.Е. Основы криптологии. (Учебное пособие)- Т.: Университет, 2004.-136 с.
8. Арипов М., Пудавченко Ю.Е., Арипов К.М. Основы Интернет. (Учебное пособие)- Т.: Университет, 2002.-195 с.
9. Аскеров Т.М. Защита информации и информационная безопасность: (Учебное пособие). Под общ. ред. К.И.Курбакова. – М.: Изд. Рос.экон. акад., 2001.–387 с.
10. Информационно-правовая система NORMA. Инструкция для пользователя. Т.: 2002. / "NORMA" huquqiy axborot qidiruv tizimi.
11. Д. Иргашева Компьютер тармоқларининг ҳимояланишини оширувчи фойдаланишни ролли чеклашли структуравий усуллар/ автореферат.- Т. «ТАТУ», 2012.
12. С.Ғаниев, М, Каримов, К.Ташев АХБОРОТ ХАВФСИЗЛИГИ.- Т. «ТАТУ», 2012