ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АЛОҚА, АХБОРОТЛАШТИРИШ ВА ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ДАВЛАТ ҚЎМИТАСИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

АХБОРОТ ХАФСИЗЛИГИ НАЗАРИЯСИ ВА МЕТОДОЛОГИЯСИ

фанидан

РЕФЕРАТ

Мавзу: Компьютер тизимларига бўладиган таҳдидлар

Бажарди: Юсупов Б.К. 509-10 ГР.

Текширди: Доц. Ганиев А.А.

Тошкент - 2013

Мавзу: Компьютер тизимларига бўладиган таҳдидлар

Режа:

Кириш

1. Компьютер тизимларига таҳдид тушунчаси
2. Тармоқ трафигини тахлиллаш
3. Тармоқнинг ёлғон объектини киритиш
4. Ёлғон маршрутни киритиш
5. Хизмат қилишдан воз кечишга ундайдиган тақсимланган ҳужумлар

Хулоса

Фойдаланилган адабиётлар

Кириш

Барча ҳужумлар компьютер тармоғининг ишлаши принципларининг қандайдир чегараланган сонига асосланганлиги сабабли масофадан бўладиган намунавий ҳужумларни ажратиш ва уларга қарши қандайдир комплекс чораларни тавсия этиш мумкин. Бу чоралар, ҳақиқатан, тармоқ хавфсизлигини таъминлайди.

Тармоқ технологиялари ривожининг бошланғич босқичида вируслар ва компьютер ҳужумларининг бошқа турлари таъсиридаги зарар кам эди, чунки у даврда дунё иқтисодининг ахборот технологияларига боғликлиги катта эмас эди. Хозирда, ҳужумлар сонининг доимо ўсиши хамда бизнеснинг ахборотдан фойдаланиш ва алмашишнинг электрон воситаларига боғликлиги шароитида машина вақтининг йўқолишига олиб келувчи хатто озгина ҳужумдан келган зарар жуда катта рақамлар орқали ҳисобланади. Мисол тариқасида келтириш мумкинки, фақат 2011 йилнинг биринчи чорагида дунё миқёсидаги йўқотишлар 2010 йилдаги барча йўқотишлар йиғиндисининг 50%ини ташкил этган, ёки бўлмаса 2013 йилнинг ўзида Россия Федереациясида 30 мингдан ортиқ компьютер жиноятчилиги холатлари кайд этилган.

Internet протоколларининг мукаммал эмаслиги сабабали тармокдаги ахборотга масофадан бўладиган асосий намунавий ҳужумлар қуйидагилар:

- тармоқ трафигини таҳлиллаш;
- тармоқнинг ёлғон обьектини киритиш;
- ёлғон маршрутни киритиш;
- хизмат қилишдан воз кечишга ундайдиган ҳужумлар.

1. Компьютер тизимларига таҳдид тушунчаси

Компьютер тизимларига таҳдид деганда тармоқдаги ахборотнинг бузилиши ёки йўқотилиши хавфига олиб келувчи ҳимояланувчи объектга қарши қилинган ҳаракатлар тушунилади.

Корпоратив тармоқларда ишланадиган ахборот, айниқса, заиф бўлади. Ҳозирда рухсатсиз фойдаланишга ёки ахборотни модификациялашга, ёлғон ахборотнинг муомалага кириши имконининг жиддий ошишига қуйидагилар сабаб бўлади:

- компьютерда ишланадиган, узатиладиган ва сақланадиган ахборот ҳажмининг ошиши;
- маълумотлар базасида муҳимлик ва маҳфийлик даражаси турли бўлган ахборотларнинг тўпланиши;
- маълумотлар базасида сақланаётган ахборотдан ва ҳисоблаш тармоқ ресурларидан фойдаланувчилар доирасининг кенгайиши;
- масофадаги ишчи жойлар сониниг ошиши;
- фойдаланувчиларни боғлаш учун Internet глобал тармоғини ва алоқанинг турли каналларини кенг ишлатиш;
- фойдалувчилар компьютерлари ўртасида ахборот алмашинувининг автоматлаштирилиши.

Ахборот хавфсизлигига тахдид деганда ахборотнинг бузилиши ёки йўқотилиши хавфига олиб келувчи ҳимояланувчи объектга қарши қилинган харакатлар тушунилади. Олдиндан шуни айтиш мумкинки, сўз барча ахборот хусусида эмас, балки унинг фақат, мулк эгаси фикрича, коммерция қийматига эга бўлган қисми хусусида кетяпти.

Замонавий корпоратив тармоқлар ва тизимлар дучор бўладиган кенг тарқалган тахдидларни таҳлил қиламиз. Ҳисобга олиш лозимки, хавфсизликка тахдид манбалари корпоратив ахборот тизимининг ичида (ички манба) ва унинг ташқарисида (ташқи манба) бўлиши мумкин. Бундай ажратиш тўғри, чунки битта тахдид учун (масалан, ўғирлаш) ташқи ва ички

манбаларга қарши харакат усуллари турлича бўлади. Бўлиши мумкин бўлган тахдидларни хамда корпоратив ахборот тизимининг заиф жойларини билиш хавфсизликни таъминловчи энг самарали воситаларни танлаш учун зарур ҳисобланади.

Тез-тез бўладиган ва хавфли (зарар улчами нуктаи назаридан) тахдидларга фойдаланувчиларнинг, операторларнинг, маъмурларнинг ва корпоратив ахборот тизимларига хизмат кўрсатувчи бошқа шахсларнинг атайин қилмаган хатоликлари киради. Баъзида бундай хатоликлар (нотўғри киритилган маълумотлар, дастурдаги хатоликлар сабаб бўлган тизимнинг тўхташи ёки бузилиши) тўғридан - тўғри зарарга олиб келади. Баъзида улар нияти бузуқ одамлар фойдаланиши мумкин бўлган нозик жойларни пайдо бўлишига сабаб бўлади. Глобал ахборот тармоғида ишлаш ушбу омилнинг етарлича долзарб қилади. Бунда зарар манбани ташкилотнинг фойдаланувчиси ҳам, Тармоқ фойдаланувчиси ҳам бўлиши мумкин, охиргиси айниқса хавфли.

Зарар ўлчами бўйича иккинчи ўринни ўғирлашлар ва сохталаштиришлар эгаллайди. Текширилган холатларнинг аксариятида ишлаш режимлари ва ҳимоялаш чоралари билан аъло даражада таниш бўлган ташкилот штатидаги ходимлар айбдор бўлиб чиқдилар. Глобал тармоқлар билан боғланган қувватли ахборот каналининг мавжудлигида, унинг ишлаши устидан етарлича назорат йўққлиги бундай фаолиятга қўшимча имкон яратади.

Хозирда ташқи коммуникация орқали рухсатсиз фойдаланишга атай-ин қилинган уринишлар бўлиши мумкин бўлган барча бузилишларнинг 10%ини ташкил этади. Бу катталик анчагина бўлиб туюлмаса хам, Internetда ишлаш тажрибаси кўрсатадики, қарийб хар бир Internet-сервер кунига бир неча марта суқилиб кириш уринишларига дучор бўлар экан. Хавф-хатарлар тахлил қилинганида ташкилот корпоратив ёки локал тармоғи компьютерларининг ҳужумларга қарши туриши ёки булмаганида ахборот хавфсизлиги бузилиши фактларини кайд этиш учун етарлича

ҳимояланмаганлигини ҳисобга олиш зарур. Масалан, ахборот тизимларини хдмоялаш Агентлигининг (АҚШ) тестлари курсатадики, 88% компьютерлар ахборот хавфсизлиги нук,таи назаридан нозик жойларга эгаки, улар рухсатсиз фойдаланиш учун фаол ишлатишлари мумкин. Ташкилот ахборот тузилмасидан сасофадан фойдаланиш холлари алохида курилиши лозим.

Ҳимоя сиёсатини тузишдан аввал ташкилотда компьютер муҳити дучор бўладиган хавф-хатар бахоланиши ва зарур чоралар кўрилиши зарур. Равшанки, химояга тахдидни назоратлаш ва зарур чораларни кўриш учун ташкилотнинг сарф-харажати ташкилотда активлар ва ресурсларни ҳимоялаш бўйича хеч қандай чоралар кўрилмаганида кутиладиган йўқотишлардан ошиб кетмаслиги шарт.

Умуман олганда, ташкилотнинг компьютер муҳити икки хил хавф - хатарга дучор бўлади:

1. Маълумотларни йўқотилиши ёки ўзгартирилиши.
2. Сервиснинг тўхтатилиши.

Таҳдидларнинг манбаларини аниқлаш осон эмас. Улар нияти бузуқ, одамларнинг бостириб киришидан то компьютер вирусларигача турланиши мумкин.

Бунда инсон хатоликлари хавфсизликка жиддий тахдид ҳисобланади. 1-расмда корпоратив ахборот тизимида хавфсизликнинг бузилиш манбалари бўйича статистик маълумотларни тасвирловчи айланма диаграмма келтирилган.

1-расм. Хавфсизликнинг бузилиш манбалари

1-расмда келтирилган статистик маълумотлар ташкилот маъмуриятига ва ходимларига корпоратив тармоқ ва тизими хавфсизлигига тахдидларни самарали камайтириш учун харакатларни қаерга йўналтиришлари зарурлигини айтиб бериши мумкин. Албатта, физик хавфсизлик муаммолари билан шуғулланиш ва инсон хатоликларининг хавфсизликка салбий таъсирини камайтириш бўйича чоралар кўрилиши зарур. Шу билан бир қаторда корпоратив Тармоқ ва тизимга ҳам ташқаридан, хам ичкаридан бўладиган ҳужумларни олдини олиш бўйича тармоқ хавфсизлиги масаласини ечишга жиддий эътиборни қаратиш зарур.

Тасодифий тахдидлар

Максадли харакатларга боглик булмаган, кандайдир вактларларда содир буладиган хавфлар тасодифий тахдидлар деб аталади.

Мақсадли тахдидлар

Иккинчи гурух ахборот хавфсизлигига хавфлар – максадли тахдидлардир. Максадли тарзда яратиладиган тахдидлар, хали етарлича урганилмаган, чунки ушбу тахдидлар жуда харакатчан ва доимий равишда янги хавфлар билан тулиб туради.

Мақсадли тахдидлар таркиби

Ушбу гурухдаги тахдидлар физик мохияти ва механизмлари амалга ошириши буйича бешта гурухга булинади

- анъанавий жосуслик ва купорувчилик;
- ахборотдан рухсатсиз фойдаланиш;
- электромагнит нурланиш ва таъсирлар;
- тизимга рухсатсиз кириш;
- зарарли дастурлар;

Зарарли дастурлар

- Ахборот хавфсизлигига тахдидлар манбаларининг энг асосийларидан бири махсус ишлаб чикилган зарарли дастурлар хисобланади.
- Ўзининг механизмлари харакати буйича зарарли дастурлар туртта гурухга булинади.
- «мантикий бомбалар»;
- «куртлар»;
- «троян отлари»;
- «компьютер вируслари».

2. Тармоқ трафигини таҳлиллаш

Сервердан Internet тармоғи базавий протоколлари FTP (File Transfer Protocol) ва TELNET (Виртуал терминал протоколи) бўйича фойдаланиш учун фойдаланувчи *идентификация* ва *аутентификация* муолажаларини ўтиши лозим. Фойдаланувчини идентификациялашда ахборот сифатида унинг идентификатори (исми) ишлатилса, аутентификациялаш учун *парол* ишлатилади. FTP ва TELNET протоколларининг хусусияти шундаки, фойдалувчиларнинг пароли ва идентификатори тармоқ орқали очиқ, шифрланмаган кўринишда узатилади. Демак, Internet хостларидан фойдаланиш учун фойдаланувчининг исми ва паролини билиш кифоя.

Ахборот алмашинувида Internetнинг масофадаги иккита узели

алмашинув ахборотини *пакетларга* бўлишади. Пакетлар алоқа каналлари орқали узатилади ва шу пайтда ушлаб қолиниши мумкин.

FTP ва TELNET протоколларининг тахлили кўрсатадики, TELNET паролни символларга ажратади ва паролнинг ҳар бир символини мос пакетга жойлаштириб битталаб узатади, FTP эса, аксинча, паролни бутунлайича битта пакетда узатади. Пароллар шифрланмаганлиги сабабли пакетларнинг махсус сканер-дастурлари ёрдамида фойдаланувчининг исми ва пароли бўлган пакетни ажратиб олиш мумкин. Худди шу сабабли, ҳозирда оммавий тус олган ICQ дастури ҳам ишончли эмас. ICQнинг протоколлари ва

ахборотларни сақлаш, узатиш форматлари маълум ва демак, унинг трафиги ушлаб қолиниши ва очилиши мумкин.

Асосий муаммо алмашинув протоколида. Базавий татбиқий проколларнинг TCP/IP оиласи анча олдин (60 йилларнинг охири ва 80-йилларнинг боши) ишлаб чиқилган ва ундан бери умуман ўзгартирилмаган. Ўтган давр мобайнида тақсимланган тармоқ хавфсизлигини таъминлашга ёндашиш жиддий ўзгарди. Тармоқ уланишларини ҳимоялашга ва трафикни шифрлашга имкон берувчи ахборот алмашинувининг турли протоколлари ишлаб чиқилди. Аммо бу протоколлар эскиларининг ўрнини олмади (SSL бундан истисно) ва стандарт мақомига эга бўлмади. Бу протоколларининг стандарт бўлиши учун эса тармоқдан фойдаланувчиларнинг барчаси уларга ўтишлари лозим. Аммо, Internetда тармоқни марказлашган бошқариш бўлмаганлиги сабабли бу жараён яна кўп йиллар давом этиши мумкин.

3. Тармоқнинг ёлғон объектини киритиш

Ҳар қандай тақсимланган тармоқда қидириш ва адреслаш каби "нозик жойлари" мавжуд. Ушбу жараёнлар кечишида тармоқнинг ёлғон объектини (одатда бу ёлғон хост) киритиш имконияти туғилади. Ёлғон обьектнинг киритилиши натижасида адресатга узатмоқчи бўлган барча ахборот аслида нияти бузуқ одамга тегади.

Тахминан буни тизимингизга, одатда электрон почтани жўнатишда фойдаланадиган провайдерингиз сервери адреси ёрдамида киришга кимдир уддасидан чиққани каби тасаввур этиш мумкин. Бу ҳолда нияти бузуқ одам унчалик қийналмасдан электрон хат-хабарингизни эгаллаши, мумкин, сиз эса ҳатто ундан шубхаланмасдан ўзингиз барча электрон почтангизни жўнатган бўлар эдингиз.

Қандайдир хостга мурожаат этилганида адресларни махсус ўзгартиришлар амалга оширилади (IP-адресдан тармоқ адаптери ёки маршрутизаторининг физик адреси аниқланади). Internetда бу муаммони ечишда ARP(Adress Resolution Protocol) протоколидан фойдаланилади.

Бу қуйидагича амалга оширилади: тармоқ ресурсларига биринчи мурожаат этилганида хост кенг кўламли ARP-сўровни жўнатади.

Бу сўровни тармоқнинг берилган сегментидаги барча станциялар қабул қилади. Сўровни қабул қилиб, хост сўров юборган хост хусусидаги ахборотни ўзининг ARP-жадвалига киритади, сўнгра унга ўзининг Ethernet адреси бўлган ARP-жавобни жўнатади. Агар бу сегментда бундай хост бўлмаса, тармоқнинг бошқа сегментларига мурожаатга имкон берувчи маршрутизаторга мурожаат қилинади. Агар фойдаланувчи ва нияти бузуқ одам бир сегментда бўлса, ARP-сўровни ушлаб қолиш ва ёлғон ARP жавобни йўллаш мумкин бўлади. Бу усулнинг таъсири фақат битта сегмент билан чегараланганлиги тасалли сифатида хизмат қилиши мумкин.

ARP билан бўлган холга ўхшаб DNS-сўровни ушлаб қолиш йўли билан Internet тармоғига ёлғон DNS-серверни киритиш мумкин.

Бу қуйидаги алгоритм бўйича амалга оширилади:

1. DNS-сўровни кутиш.

2. Олинган сўровдан керакли маълумотни чиқариб олиш ва тармоқ бўйича сўров юборган хостга ёлғон DNS-жавобни ҳақиқий DNS сервер номидан узатиш. Бу жавобда ёлғон DNS-сервернинг IP адреси кўрсатилган бўлади.

3. Хостдан пакет олинганида пакетнинг IP-сарлавхасидаги IP-адресни

ёлғон DNS серверининг IP-адресига ўзгартириш ва пакетни серверга узатиш (яъни ёлғон DNS-сервер ўзининг номидан сервер билан иш олиб боради).

4. Сервердан пакетни олишда пакетнинг IP-сарлавҳасидаги IP адресни ёлғон DNS-серверининг IP-адресига ўзгартириш ва пакетни хостга узатиш (ёлғон DNS серверни хост ҳақиқий ҳисоблайди).

4. Ёлғон маршрутни киритиш

Маълумки, замонавий глобал тармоқлари бир-бири билан *тармоқ узеллари* ёрдамида уланган тармоқ сегментларининг мажмуидир. Бунда *маршрут* деганда маълумотларни манбадан қабул қилувчига узатишга хизмат қилувчи тармоқ узелларининг кетма-кетлиги тушунилади. Маршрутлар хусусидаги ахборотни алмашишни унификациялаш учун маршрутларни бошқарувчи махсус протоколлар мавжуд. Internetдаги бундай протоколларга янги маршрутлар хусусида хабарлар алмашиш протоколи — ICMP (Internet Control Message Protocol) ва маршрутизаторларни масофадан бошқариш протоколи SNMP (Simple Network Manegment Protocol) мисол бўла олади. Маршрутни ўзгартириш ҳужум қилувчи ёлғон хостни киритишдан бўлак нарса эмас. Ҳатто охирги обьект ҳақиқий бўлса, ҳам маршрутни ахборот барибир ёлғон хостдан ўтадиган қилиб қуриш мумкин.

Маршрутни ўзгартириш учун ҳужум қилувчи тармоққа тармоқни бошқарувчи қурилмалар (масалан, маршрутизаторлар) номидан берилган тармоқни бошқарувчи протоколлар орқали аниқланган махсус хизматчи хабарларни жўнатиши лозим. Маршрутни муваффаққиятли ўзгартириш натижасида ҳужум қилувчи тақсимланган тармоқдаги иккита обьект алмашадиган ахборот оқимидан тўла назоратга эга бўлади, сўнгра ахборотни ушлаб қолиши, таҳлиллаши, модификациялаши ёки оддийгина йўқотиши мумкин. Бошқача айтганда таҳдидларнинг барча турларини амалга ошириш имконияти туғилади.

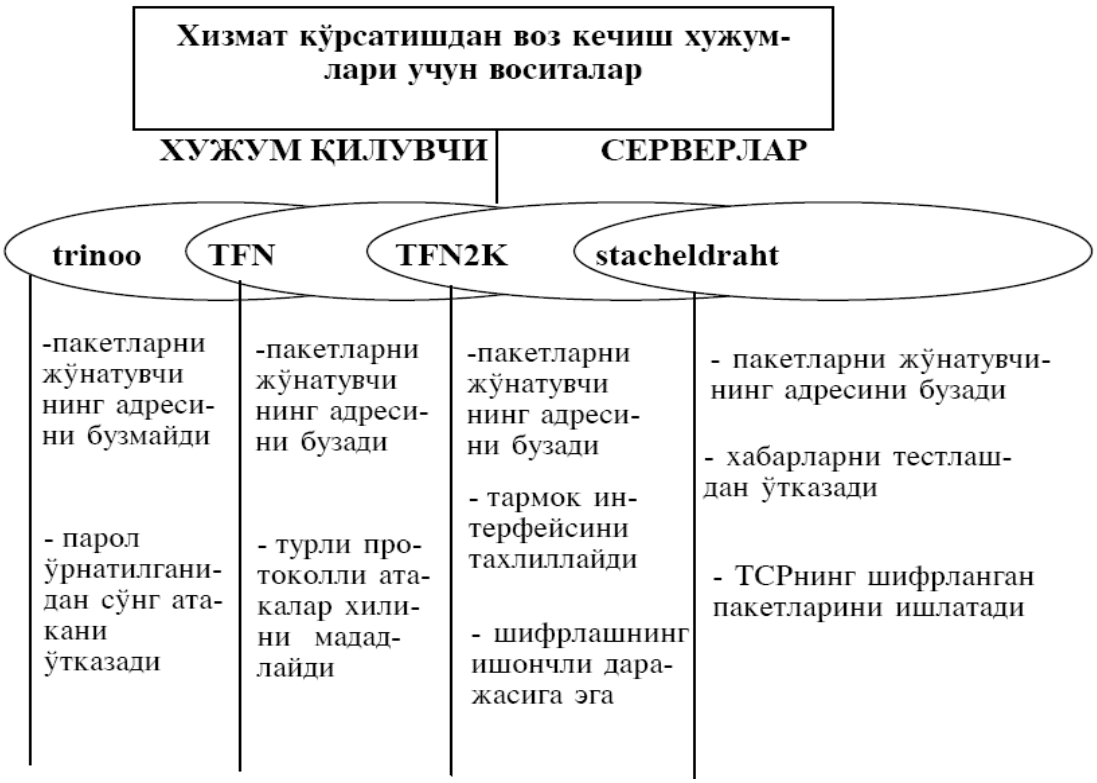
5. Хизмат қилишдан воз кечишга ундайдиган тақсимланган ҳужумлар

Хизмат қилишдан воз кечишга ундайдиган тақсимланган ҳужумлар — DdoS (Distributed Denial of Service) компьютер жиноятчилигининг нисбатан янги хили бўлсада, қўрқинчли тезлик билан тарқалмоқда. Бу ҳужумларнинг ўзи анчагина ёқимсиз бўлгани етмаганидек, улар бир вақтнинг ўзида масофадан бошқарилувчи юзлаб хужум қилувчи серверлар томонидан бошланиши мумкин.

Хакерлар томонидан ташкил этилган узелларда DDoS ҳужумлар учун учта инструментал воситани топиш мумкин: trinoo, Tribe FloodNet (TFN) ва TFN2K. Яқинда TFN ва trinoo нинг энг ёқимсиз сифатларини уй ўзлаштирган яна биттаси stacheldraht ("тикон симлар") пайдо бўлди.

2-расмда хизмат қилишдан воз кечишга ундайдиган ҳужум воситаларининг характеристикалари келтирилган.

Хизмат қилишдан воз кечишга ундайдиган оддий тармоқ ҳужумида хакер танлаган тизимига пакетларни жўнатувчи инструментидан фойдаланади. Бу пакетлар нишон тизимининг тўлиб тошиши ва бузилишига сабаб бўлиши керак. Кўпинча бундай пакетларни жўнатувчилар адреси бузиб кўрсатилади. Шу сабабли ҳужумнинг ҳақиқий манбасини аниқлаш жуда қийин.



2-расм. Хизмат қилишдан воз кечишга ундайдиган ҳужум воситалари

Хулоса

Компьютер тизимларида таҳдид тушунчаси учта категорияга бўлиниб – ахборот ресурсларига, дастурий таъминотга ва техник воситаларга (файл серверлари, ишчи станциялар, кўприқлар, маршрутизаторлар ва ҳ.) бўлинади. Ҳар бир категория ичида ресурсларни синфларга ва қисм синфларга ажратиш мумкин. Фақат корпоратив ахборот тизими функционаллигини белгиловчи ва хавфсизликни таъминлаш нуқтаи назаридан муҳим бўлган ресурлар идентификацияланиши лозим.

Ресурснинг муҳимлиги (нархи) бу ресурснинг конфиденциаллиги, яхлитлиги ёки фойдаланувчанлиги бузилганида етказилган зарар миқдори билан белгиланади. Ресурслар нархини баҳолашда ресурсларининг ҳар бир категорияси учун бўлиши мумкин бўлган зарар миқдори белгиланади.

Намунавий хавфсизлик тахдидларига корпоратив ахборот тизими ресурсларига локал масофадан хужумлар, табиий офат, ходимлар хатоси, дастурий таъминотдаги хатолик ёки аппаратуранинг носозлиги сабаб бўлувчи корпоратив ахборот тизим ишидаги бузилишлар тааллуқли. Тахдид даражаси деганда унинг амалга оширилиши эҳтимоллиги тушунилади.

Фойдаланилган адабиётлар

1. С.К. Ғаниев, М.М. Каримов, К.А. Ташев Ахборот хавфсизлиги. “ ALOQACHI” – 2008.
2. Васильков А. В. Васильков А. А. Васильков И. А. Информационные системы и их безопасность. Москва-2011.
3. В. П. Мельников, С. А. Клейменов, А. М. Петраков Информационная безопасность и защита информации. Москва Издательский центр “Академия” -2009
4. Васильков А. В. Васильков И. А Безопасность и управление доступен в информационных системах. Москва-2010.
5. В. Ф. Шаньгин Комплексная защита информации в корпоративных системах. Москва ИД “ФОРУМ” – ИНФРА-М 2010.