13-зертханалық жұмыс. **Желідегі компьютердің қауіпсіздігін қамтамасыз ету. Қосылуларды жалпы баптау басқаруларын пайдалану**

Жұмыстың мақсаты: Желідегі қауіпсіздікті қамтамасыз ету және жүйедегі қосылуларды басқару дағдыларын қалыптастыру.
Қысқаша теориялық ақпарат. Қауіпсіздік – бұл желідегі ақпараттың жоғалуының алдын алу немесе жариялануын болдырмау үшін қолданылатын шаралар кешені. Жұмысқа жарамды жүйелердегі жоғалту ықтималдығын толығымен жою мүмкін емес, белгілі бір дәрежеде қауіп-қатер тәуекелі орын алуы заңдылық және жүйенің қауіпсіздігі тек сенімді қауіпсіздік қағидаларына негізделген қол жетімділікті (тұтынушыларға немесе компьютерлерге) қамтамасыз етуге негізделуі керек.
Қауіпсіздікті басқару үшін кез-келген жүйе:
• қол жетімділікті бақылауы;
• пайдаланушыларды анықтауы;
• қол жетімділікті шектеу немесе оған рұқсат беруі;
• тұтынушының әрекеттерін жазып отыруы;
• жүйелер арасындағы жабық өзара әрекеттесуді жүзеге асыруы;
• қате конфигурация қаупін барынша азайтуы
керек.

Шифрлеу, математикалық алгоритмді (шифрді) пайдаланып хабарламаны жасыру үдерісі және тек құқылы тараптарға белгілі құпия мән (кілт) – барлық заманауи компьютерлік қауіпсіздіктің негізін құрайды.
Шифрлау тұтынушының жеке басын немесе компьютерді растау, деректерді тексеру немесе сақтау кезінде, байланыс ағынында мәліметтер мазмұнын жасыру үшін қолданылады.

Windowstың қауіпсіздігі тұтынушының аутентификациясына негізделген. Windows жүйесіне кіргенде тұтынушылар файлдарға, программаларға және серверлердегі ортақ деректерге қол жеткізу үшін жеке басын растайды. Windows жүйесі тіркеу деректері бойынша сәтті кіргеннен кейін тұтынушыға компьютерді кеңінен қол жетімді етудің орнына, тұтынушының барлық әрекеттерін тексеретін қауіпсіздіктің «тесіп өту» (пронизывающая) моделін қолданады.
Операциялық жүйе сенімді болуы үшін ол өзінің рұқсат етілмеген өзгерістерге ұшырамағанына және ақпараттың басқа тұтынушылардан қауіпсіз сақтала алатынына кепілдік беруге қабілетті болуы керек. Windows файлдарға, соның ішінде Windows жүйесін жүктеуді қамтамасыз ететін файлдарға қол жетімділікті басқару үшін NTFS файлдық жүйесінің шешімдері мен рұқсаттарын пайдаланады.
Рұқсаттар тұтынушылар мен тұтынушылар топтарына файлдық жүйенің әр функциясы үшін берілуі мүмкін. Файлдар оларға қол жетімділікті компьютер өшірілген кезде де қамтамасыз ету үшін дискте шифрленіп сақталуы мүмкін.
Windowstың желілік қауіпсіздігі хэштелген Kerberos құпия сөздерінің, топтық саясат пен IPSec саясаттарының репозитарий ретінде пайдаланылатын Active Directory көмегімен басқарылады. Active Directory сонымен қатар қауіпсіздік принципалдары (рұқсат берілетін объекттер) арасындағы қатынастарды анықтайды.

Windows Kerberos-ты желі арқылы тұтынушының тіркеу деректерін тексеру үшін қолданады. Kerberos – бұл үшінші тараптың сенімді қауіпсіздік жүйесі болып табылады. Өзара әрекеттесетін екі шектік нүкте де Kerberos серверіне сенімді болғандықтан, олар бір-біріне де сенеді. Kerberos серверлері басқа Kerberos серверлеріне сене алады, сондықтан үлкен қашықтыққа бөлінген желілердегі шектік нүктелер арасында айқындығы расталған өзара әрекеттесу сеанстарын орнатуға мүмкіндік беретін транзитивтік сенімді қатынастар құрылуы мүмкін. Kerberos жүйесі Active Directory-мен интеграцияланған (доменнің барлық контроллерлері Kerberos кілттерін үлестіру орталықтары – Kerberos Key Distribution Center – болып табылады) және оның бір домен ағашына қосылуы автоматты түрде транзиттік екі жақты сенімдік қатынастар тудырады.

Топтық саясаттар қауіпсіздік талаптарын орнату және домендегі, кеңседегі немесе OU контейнеріндегі компьютерлер мен тұтынушылардың тіркеу жазбаларын конфигурациялау үшін қолданылады. Топтық саясаттарды іс жүзінде компьютерлер мен тұтынушылардың барлық қауіпсіздік элменттерін басқару үшін қолдануға болады.
Топтық саясаттар Active Directoryдің Users and Computers (Пайдаланушылар және компьютерлер) жабдықшасынан (**оснастка**) Active Directory Sites and Services (сайттар мен қызметтер) жабдықтамасынан басқарылады.
IPSec – бұл Интернеттің IP-дестелердің шынайылығын қамтамасыз етуге және IP-дестелерге салынған деректерді шифрлауға арналған стандарты. IPSec көптеген түрлі қауіпсіздік алгоритмдерімен жұмыс істейді және қалыпты көлік режимінде немесе Интернет сияқты ашық желідегі жабық арнаны эмуляциялау үшін туннель режимінде жұмыс істей алады.
Интернет дәуіріндегі қауіпсіздік дегеніміз – белгісіз компьютерлерден тарайтын сессияларды белсенді түрде бұғаттау, тұтынушыларды ашық шифрлау кілттерінің сертификаттары негізінде авторлау, файлдар мен каталогтарды пайдалануды тексеру, деректерді тасымалдауды шифрлау және құқылы тұтынушылардың вирустар мен трояндық аттарды кездейсоқ белсендіруіне жол бермеу.
Нашар дайындалған Windows NT4-тен сабақ ала отырып, Windows тұтынушыларды аутентификациялау, деректерді шифрлеу, қауіпсіз қосылуларды қамтамасыз ету, рұқсатсыз қол жеткізулерге тыйым салу және қауіпсіздікті тұтастай басқару сияқты күрделі құралдар жиынтығын ұсынады. Үнсіз келісім бойынша қызметтер жиынтығы көмегімен Windowsты кез-келген басқа бұқаралық нарыққа арналған негізгі операциялық жүйелерге қарағанда көбірек қауіпсіз етуге болады – соның ішінде UNIXтің немесе Linuxтің барлық нұсқаларына қарағанда – және басқару және қауіпсіз күйде пайдалану оңайырақ. Соған қарамастан Windows бәрін алдын ала ескере алмайды, өйткені Microsoft және басқа үшінші тараптағы программалық жасақтама жеткізушілері Internet Explorer, Outlook және Office сияқты тұтынушылық өнімдердің қауіпсіздігінен гөрі пайдаланудың қарапайымдылығына басымдық береді.
Бұл бағдарламалардың барлығында желі әкімшілерінен үнемі қырағылықты талап ететін олардың сценарийлік кіріктірілген процессорлары болғандықтан, қауіпсіздіктегі елеулі кемшіліктер бар. Windows сонымен қатар осы мәселелерді шешуге көмектесе алады. Бірақ Майкрософт өзінің тұтынушылар үшін құрылған

соңғы өнімдерінде қауіпсіздікке аса көңіл бөле қоймайды, сондықтан сіздің желіңіздегі осы бағдарламалардан туындаған қауіпсіздік мәселелерін болдырмаудың жалғыз жолы – оларды мүлдем пайдаланбау.
Windows XP операциялық жүйесінің SP2 әкімшілік шаблондарына қосымша параметрлер қосылған. Бұл параметрлерді баптау үшін барлық GPO жаңа Windows XP SP2 әкімшілік шаблондары көмегімен жаңартылуы керек. Кері жағдайда, Windows брандмауэрін баптау параметрлері қол жетімді болмайды.
Windows XP SP2 операциялық жүйесінің басқаруымен жұмыс істейтін компьютерлерде GPO объектілерін Топтық саясат объектілері редакторы (Group Policy Object Editor) жабдықшасы (**оснастка**) орнатылған Microsoft басқару консолі (Microsoft Management Console – MMC) көмегімен жаңартуға болады.
GPO объектілерін жаңартқаннан кейін Сіз Windows XP SP2 операциялық жүйесі басқаруымен жұмыс істейтін компьютерлер үшін брандмауэр параметрлерін баптай аласыз.

Қауіпсіздікті қамтамасыз ету орталығы параметрлерін баптау
Осы тапсырманы орындауға қойылатын талаптар
• **Тіркеу деректері:** Сіздің **Домен әкімшілері** немесе **Топтық саясатты құрушы-иелер** қауіпсіздік тобының мүшесі ретінде домен құрамында Windows XP SP2 операциялық жүйесі басқаруымен жұмыс істейтін компьютердегі жүйеге кіруіңіз керек.
• **Құралдар:** Топтық саясат объектілері редакторы (Group Policy Object Editor) жабдықтамасы орнатылған Microsoft басқару консолі (Microsoft Management Console – MMC).
Қауіпсіздікті қамтамасыз ету орталығы – бұл Windows XP SP2 ОЖ-ң қауіпсіздік параметрлерін баптаудың біртұтас нүктесін қамтамасыз ететін, компьютер қауіпсіздігі туралы қосымша ақпарат беретін және Microsoft корпорациясының қазіргі ұсынған қауіпсіздік талаптарына сәйкестігін бақылауға мүмкіндік беретін жаңа қызметі.
Windows домендік ортасында Сіз Топтық саясатты Қауіпсіздікті қамтамасыз ету орталығын қосу, клиенттердің компьютерлеріне қауіпсіздіктің соңғы жаңартулары орнатылғанын мониторинг жасау мақсатында және тұтынушыларға компьютерлеріне қауіп төнген кезде хабарлау үшін қолдана аласыз.
Қауіпсіздікті қамтамасыз ету орталығы қызметі фондық процесс ретінде жұмыс істейді және тұтынушы компьютеріндегі келесі компоненттердің күйін тексереді:
• **Брандмауэр**. Қауіпсіздікті қамтамасыз ету орталығы Windows брандмауэрінің қосылуын және басқа программалық брандмауэрлардың бар-жоғын тексереді. Басқа брандмауэрлерді тексеру үшін Қауіпсіздікті қамтамасыз ету орталығы программалық жасақтама құрушыларға қол жетімді Windowsты басқару құрал-саймандарын (Windows Management Instrumentation – WMI) арнайы жеткізушілеріне сұрау салады.
• **Вирустардан қорғау**. Қауіпсіздікті қамтамасыз ету орталығы вирусқа қарсы программалық жасақтаманы тексереді. Ол үшін қауіпсіздік орталығы программалық жасақтама жасаушыларға қол жетімді Windows Management Instrumentation арнайы провайдерлеріне сұраныстар жасайды. Егер қажетті ақпарат болса, қауіпсіздік

орталығы орнатылған жаңартулар мен антивирустық сканердің мәртебесін (статус) де тексереді.

• **Автоматты түрде жаңарту**. Қауіпсіздікті қамтамасыз ету орталығы автоматты түрде жаңарту параметрлерінің талап етілетін параметрлерге сәйкес келетіндігін тексереді, бұл маңызды жаңартулардың автоматты түрде жүктелуін және клиенттік компьютерлерде орнатылуын қамтамасыз етеді. Егер автоматты түрде жаңарту өшіріліп тұрса немесе белгіленген параметрлерге сәйкес келмесе, Қауіпсіздікті қамтамасыз ету орталығы тиісті ұсыныстарды жасайды.

Егер осы компоненттердің кез-келгені жоқ болса немесе сіздің қауіпсіздік саясатыңызға сәйкес келмесе, Қауіпсіздікті қамтамасыз ету орталығы тұтынушыға есептер тақтасындағы хабарландыру аймағында қызыл белгіше көмегімен хабарлама береді, сонымен қатар жүйеге кірген кезде ескерту жасайды. Ескертуде Қауіпсіздікті қамтамасыз ету орталығына сілтеме жасалып, туындаған мәселе туралы ақпарат пен оны шешуге байланысты ұсыныстар жазылады.

Егер Қауіпсіздікті қамтамасыз ету орталығы анықтай алмайтын брандмауэр немесе антивирустық программа қолданылса, онда бұл компоненттер үшін ескерту хабарламаларын басып шығаруды алып тастауға болады.

Windows домені құрамындағы компьютерлерде Қауіпсіздікті қамтамасыз ету орталығының параметрлерін орталықтан басқару үшін топтық саясат параметрлерін пайдалануға болады.

Егер Топтық саясаттың **«Қауіпсіздікті қамтамасыз ету орталығын» қосу (тек домендегі компьютерлер үшін)** параметрі қосылса, онда бұл Қауіпсіздікті қамтамасыз ету орталығы негізгі қауіпсіздік параметрлерін (брандмауэр, антивирус және автоматты түрде жаңартулар) бақылайды және тұтынушыларға олардың компьютерлеріне қауіп төніп тұрғаны туралы хабарлайды дегенді білдіреді. Үнсіз келісім бойынша **Қауіпсіздікті қамтамасыз ету орталығын қосу (тек домендегі компьютерлер үшін)** параметрі тағайындалмаған, демек ол өшірілген. Егер Қауіпсіздікті қамтамасыз ету орталығы өшірілсе, хабарламалар да, күй бөлімі де көрсетілмейді.

Қауіпсіздікті қамтамасыз ету орталығы параметрлерін баптау

Осы тапсырманы орындауға қойылатын талаптар

• **Тіркеу деректері:** Сіз домен құрамында Windows XP SP2 операциялық жүйесі басқаруымен жұмыс істейтін компьютердегі жүйеге **Домен әкімшілері** қауіпсіздік тобының мүшесі ретінде кіріп, қажет Топтық саясат объектін (GPO) ашыңыз.

• **Құралдар:** Топтық саясат объектілері редакторы (Group Policy Object Editor) жабдықтамасы орнатылған Microsoft басқару консолі (Microsoft Management Console – MMC).

Бұл параметрлерді Windows Windows XP SP2 операциялық жүйесі басқаруымен жұмыс істейтін компьютерлер тұтынушыларына Қауіпсіздікті қамтамасыз ету орталығын брандмауэр, антивирустық бағдарламалар мен автоматты жаңартулардың күйін бақылауға рұқсат беру үшін пайдаланыңыз.

Windows XP SP2 ОЖ компьютердің және тұтынушы конфигурациясының Internet Explorer шолушысының барлық қауіпсіздік параметрлерін жаңа Топтық саясаттың жаңа параметрлері көмегімен басқаруға мүмкіндік береді.

Windows XP SP2 саясат параметрлерінің екі негізгі бөлімін қолданады:

• Қауіпсіздік құралдары;
• Қауіпсіздік аймақтары.

Қауіпсіздік құралдары бөлімінің параметрлері Internet Explorer шолушысының қауіпсіздігіне әсер етуі мүмкін ерекше сценарийлерді басқаруға мүмкіндік береді. Көп жағдайда Сіз белгілі бір салдардың алдын алғыңыз келуі мүмкін, сондықтан қауіпсіздік функциялары қосылғанына сенімді болуыңыз керек. Мысалы, Интернет аймағының орнына Жергілікті компьютер аймағында іске қосылған зиянды код өз ықпалын арттыруға тырысуы мүмкін. Мұндай шабуылдардың алдын алу үшін Сіз Топтық саясаттың **Аймақ деңгейін көтеруден қорғау** бөліміндегі параметрлерін қолдана аласыз.

Қауіпсіздік құралдары саясатының әр параметрі үшін саясат параметрлері кіретін және қауіпсіздік құралдарының қасиеттерін басқаратын келесі үдерістерді көрсете аласыз:
• Internet Explorer үдерістері;
• Үдерістер тізімі;
• Қай жерден іске қосылғанынан тәуелсіз барлық үдерістер.

URLды баптау бөлімінің параметрлері шолушының (браузердің) компьютерге зиян тигізуге қабілетті, мысалы, **Java** апплетін немесе **ActiveX** басқару элементін іске қосу сияқты, әрекеттерін бақылауға мүмкіндік береді. URL параметрлерін баптау бөлімі берілген URL-мекенжайға сәйкес келетін қауіпсіздік аймағындағы осы қасиеттерге арналған әрекеттерді анықтайтын тізілімдегі (реестрдегі) қауіпсіздік параметрлерімен байланысты. URLды баптау параметрлері Қосу, Ажырату, Сұраныс жасау (Enable, Disable, Prompt) мәндеріне ие және параметрден тәуелді қосымша мәндерді де қабылдай алады.

URL баптау параметрлерін басқару үшін Internet Explorerде **Шолушыны басқару тақтасында** жиналған Топтық саясаттың жаңа параметрлері қолданылады. Топтық саясат көмегімен URL баптауларын анықтап, Сіз ұйымдағы барлық тұтынушылар мен компьютерлер үшін Internet Explorer шолушысының стандартты конфигурациясын жасай аласыз.

Қауіпсіздікті қамтамасыз ету үшін Сіз барлық аймақтар үшін қауіпсіздік аймағы саясаттары шаблондары (үлгілері) көмегімен саясаттар қоса аласыз. Қауіпсіздік аймағының саясаттары шаблондарының әрқайсысы үшін Сіз келесі қауіпсіздік деңгейлерінің бірін көрсете аласыз:

• **Төменгі.** Бұл деңгей әдетте құрамында сенімді веб-тораптары бар қауіпсіздік аймағы үшін қолданылады. Бұл – **Сенімді тораптар** аймағы үшін үнсіз келісім бойынша тағайындалатын деңгей.

• **Орташадан төменгі**. Бұл деңгей сіздің компьютеріңізге қандайда бір ықтималдық үлесі бар зиян тигізуі мүмкін веб-тораптары кіретін қауіпсіздік аймағы үшін қолданыла алады. Бұл – **Жергілікті интранет** аймағы үшін үнсіз келісім бойынша тағайындалатын деңгей.

• **Орташа.** Бұл деңгей сенімді де емес және шектеусіз де емес веб-тораптарды қамтитын қауіпсіздік аймағы үшін қолданыла алады. Бұл – Интернет аймағы үшін үнсіз келісім бойынша тағайындалатын деңгей.

• **Жоғары.** Бұл деңгей Сіздің компьютеріңізге зиян келтіруі мүмкін веб-тораптары бар қауіпсіздік аймағы үшін қолданылады. Бұл – **Шектеулі тораптар** аймағы үшін үнсіз келісім бойынша тағайындалатын деңгей.

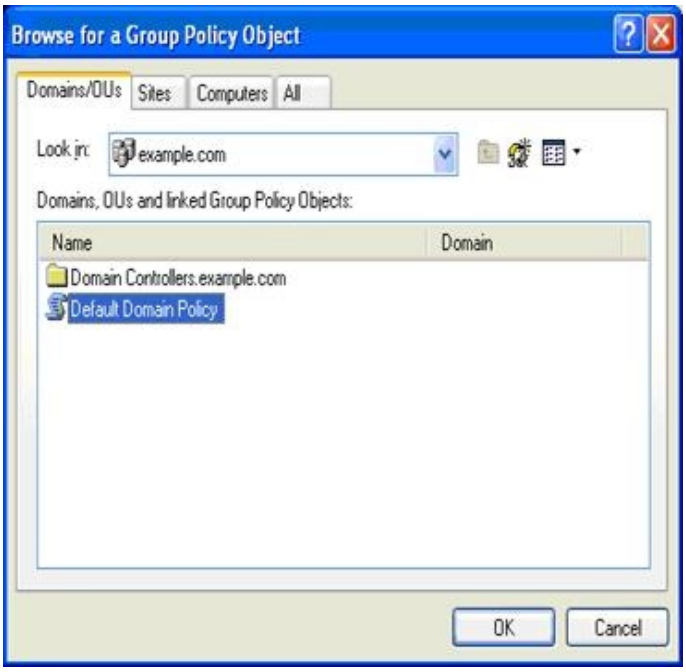
Зертханалық жұмыс орындау үдерісі. Осы тапсырманы орындауға қойылатын талаптар

• **Тіркеу деректері:** Сіз домен құрамында Windows XP SP2 операциялық жүйесі басқаруымен жұмыс істейтін компьютердегі жүйеге **Домен әкімшілері** қауіпсіздік тобының мүшесі ретінде кіріп, Топтық саясаттың қажет объектісін (GPO) ашыңыз.

• **Құралдар:** Топтық саясат объектілері редакторы (Group Policy Object Editor) жабдықтамасы орнатылған Microsoft басқару консолі (Microsoft Management Console – MMC).

1-жаттығу: Топтық саясат нысандарын жаңарту

1. **Бастау** (Пуск) батырмасын басыңыз, **Орындау** (Выполнить) мәзірін таңдап, ***mmc*** деп теріңіз және содан кейін ОК батырмасын басыңыз.
2. **Консоль** мәзірінен **Жабдықшаны қосу немесе жою** пунктін таңдаңыз.
3. **Оқшауланған жабдықша** (Изолированная оснастка) қыстырма бетінде **Қосу** (Добавить) батырмасын басыңыз.
4. **Қол жетімді оқшауланған жабдықшалар** (Доступные изолированные оснастки) тізімінен **Топтық саясат нысаны редакторы** жабдықшасын таңдап, **Қосу** (Добавить) батырмасын басыңыз.
5. **Топтық саясаттар нысанын таңдау** (Выбор объекта групповой политик) сұхбаттық терезесінде **Шолу** (Обзор) батырмасын басыңыз.



13.1-сурет. Топтық саясат объектісін таңдау

6. **Топтық саясат объектісін іздеу** (Поиск объекта групповой политики, Find GPO**)** сұхбат терезесінде Windows брандмауэрінің жаңа параметрлерін пайдалану үшін жаңартуыңыз қажет GPO нысанын көрсетіңіз.

7. Топтық саясат шебері жұмысын аяқтау үшін алдымен ОК батырмасын, сонан соң **Дайын** (Готово) батырмасын басыңыз. Мұнымен Сіз таңдалған Топтық саясат объектілеріне (GPO) жаңа әкімшілік шаблондарды қолданасыз.
8. **Оқшауланған жабдықшаны қосу** (Добавить изолированную оснастку) сұхбат терезесінде **Жабу** (Закрыть) батырмасын басыңыз.
9. **Жабдықшаны қосу немесе жою** (Добавить или удалить оснастку) сұхбат терезесінде ОК батырмасын басыңыз.
10. Консоль мәзірінен **Шығу** (Выход, Exit) пунктін таңдап, басқару консолін жабыңыз. Консоль параметрлерінің өзгерістерін сақтамаңыз.

Ескерту. *Консольдың параметрлері өзгермегенімен, жоғарыда сипатталған қадамдар Windows XP SP2 операциялық жүйесінің жаңа әкімшілік шаблондарын Топтық саясаттың көрсетілген объектілеріне (GPO) импорттайды. Үлгілерді көрсетілген барлық GPO-ға импорттау керек.*

1-тапсырма:
1. Жоғарыда келтірілген қадамдарды Windows XP SP2 жүйесі басқаруымен жұмыс жасайтын компьютерлерде Топтық саясаттары қолданылатын барлық GPO үшін қайталаңыз.

Ескерту. *Microsoft компаниясы Active Directory каталогтары мен Windows XP SP1 ОЖ қызметін қолданатын желілік ортада GPO нысандарын жаңарту үшін тегін жүктеуге болатын қол жетімді топтық саясатты басқару консолін пайдалануға кеңес береді.*

2. Орындалған жұмысты оқытушыға көрсетіңіз.

2-жаттығу: **Қауіпсіздікті қамтамасыз ету орталығы параметрлерін баптау.**
Ол үшін келесі қадамдарды орындаңыз:
1. **Бастау** (Пуск) батырмасын басыңыз, **Орындау** (Выполнить) мәзірін таңдап, ***mmc*** деп теріңіз және содан кейін ОК батырмасын басыңыз.
2. **Консоль** мәзірінен **Жабдықшаны қосу немесе жою** пунктін таңдаңыз.
3**. Оқшауланған жабдықша** (Изолированная оснастка) қыстырма бетіндегі **Қосу** (Добавить) батырмасын басыңыз.
4. **Қол жетімді оқшауланған жабдықшалар** (Доступные изолированные оснастки) тізімінен **Топтық саясат нысаны редакторы** жабдықшасын таңдап, **Қосу** (Добавить) батырмасын басыңыз.
5. **Топтық саясаттар нысанын таңдау** (Выбор объекта групповой политик) сұхбаттық терезесінде **Шолу** (Обзор) батырмасын басыңыз.
6. Тізімнен баптау керек GPO объектісін көрсетіңіз. Топтық саясат шеберінің жұмысын аяқтау үшін алдымен ОК батырмасын, сонан соң **Дайын** (Готово) батырмасын басыңыз.
7. Сұхбат терезесін жабу үшін **Оқшауланған жабдықшаны қосу** (Добавить изолированную оснастку) сұхбат терезесінде **Жабу** (Закрыть) батырмасын басыңыз.
8. Консоль ағашында **Компьютер конфигурациясы** (Конфигурация компьютера), **Әкімшілік шаблондары** (Административные шаблоны), **Windows компоненттері** (Компоненты Windows) бөлімдерін, содан кейін **Қауіпсіздікті қамтамасыз ету орталығын** ашыңыз.

9. **Қауіпсіздікті қамтамасыз ету орталығы (тек домендегі компьютерлер үшін)** – Центр обеспечения безопасности (только для компьютеров в домене) – бөліміндегі **Қосу** (Включить) параметрін екі рет басыңыз, алып-қосқышты Қосылған (**Включен)** күйіне қойып, ОК батырмасын басыңыз.

3-жаттығу: Internet Explorer үшін қауіпсіздік параметрлерін баптау

1. **Бастау** (Пуск) батырмасын басыңыз, **Орындау** (Выполнить) мәзірін таңдап, ***mmc*** деп теріңіз және содан кейін ОК батырмасын басыңыз.
2. **Консоль** мәзірінен **Жабдықшаны қосу немесе жою** пунктін таңдаңыз.
3**. Оқшауланған жабдықша** (Изолированная оснастка) қыстырма бетіндегі **Қосу** (Добавить) батырмасын басыңыз.
4. **Қол жетімді оқшауланған жабдықшалар** (Доступные изолированные оснастки) тізімінен **Топтық саясат нысаны редакторы** жабдықшасын таңдап, **Қосу** (Добавить) батырмасын басыңыз.
5. **Топтық саясаттар нысанын таңдау** (Выбор объекта групповой политик) сұхбаттық терезесінде **Шолу** (Обзор) батырмасын басыңыз.
6. Баптау керек GPO объектісін көрсетіңіз. Топтық саясат шеберін жабу үшін алдымен ОК батырмасын, сонан соң **Дайын** (Готово) батырмасын басыңыз.
7. Сұхбат терезесін жабу үшін **Оқшауланған жабдықшаны қосу** (Добавить изолированную оснастку) сұхбат терезесінде **Жабу** (Закрыть) батырмасын басыңыз, содан кейін, басқару консоліне оралу үшін ОК батырмасын басыңыз.
8. Консоль ағашында алдымен **Компьютер конфигурациясы** (Конфигурация компьютера), **Әкімшілік шаблондары** (Административные шаблоны), **Windows компоненттері** (Компоненты Windows), **Internet Explorer** бөлімдерін біртіндеп ашып, содан кейін **Қауіпсіздік құралдарын** (Средства безопасности) ашыңыз.

2-тапсырма:

1. Internet Explorer шолушысының қауіпсіздік параметрлерін баптау үшін 1-кестедегі ақпаратты пайдаланыңыз.
2. Орындалған жұмысты оқытушыға көрсетіңіз.

1-кесте

Параметр	**Сипаттама**	**Үнсіз келісім бойынша тағайындалған мән**	**Корпоративтік орта үшін ұсынылатын мән**
Қауіпсіздікті екілік кодты өңдеу үшін шектеу	Екілік кодты өңдеуге арналған қауіпсіздікті шектеуді басқару құралдары параметрі тыйым салынған немесе рұқсат етілген болуы мүмкін	Тағайындалмаған	Ұйымыңызға қажетті мәндерді әкімші рұқсат еткен әрекеттер тізіміне #package#behavior шартты белгілер пішімі түрінде қосыңыз
МК-хаттамасының қауіпсіздігін шектеу	МК-хаттамасына тыйым салу арқылы шабуылдау мүмкіндігін азайтады	Тағайындалмаған	Барлық үдерістер үшін қосылған
Жергілікті	Зиянды HTML-кодын	Тағайындалмаған	Барлық үдерістер үшін

компьютердің оқшауланған аймағының қауіпсіздігі	жүктеу үшін шабуылдың негізгі бағыты ретінде жергілікті компьютер аймағы қолданылатын кезде шабуылдарды жеңуге көмектеседі		қосылған
MIME өңдеу кезіндегі сәйкестік	Саясаттың бұл параметрі веб-серверден алынған барлық типтегі файл ақпараттарының бір біріне сәйкес келуін Internet Explorer-дің талап ететіндігін анықтайды.	Тағайындалмаған	Барлық үдерістер үшін қосылған
MIMEні сынама тексеру мүмкіндігі	Саясаттың бұл параметрі Internet Explorer көмегімен орындалатын MIME сынама тексеруінің потенциалды қауіптірек файлды өңдеудің алдын алатынын анықтайды.	Тағайындалмаған	Барлық үдерістер үшін қосылған
Кэштелетін нысандарды қорғау	Саясаттың бұл параметрі нысан сілтемесінің домен аумағында немесе жаңа доменге ауысу кезінде қол жетімді болуын анықтайды	Тағайындалмаған	Барлық үдерістер үшін қосылған
Сценарийлермен өңделетін терезелерге арналған қауіпсіздік шектеулері	Терезелерге арналған қауіпсіздік шектеулер қою мүмкіндігі қалқып шығатын терезелерге шектеулер қояды және тақырып пен күй жолағы пайдаланушыға көрінбейтін немесе басқа терезелердің тақырыбы мен күй жолағын жауып тұратын сценарийдің көрсетілуіне жол бермейді	Тағайындалмаған	Барлық үдерістер үшін қосылған
Аймақ деңгейінің көтерілуінен қорғау	Саясаттың бұл параметрі жергілікті компьютердің қауіпсіздік аймағын қорғауға көмектеседі	Тағайындалмаған	Барлық үдерістер үшін қосылған
Ақпарат тақтасы	Саясаттың бұл параметрі файлды немесе кодты орнату шектелген кезде Internet Explorer процестеріне арналған Ақпараттық тақтаның бейнеленуін басқаруға мүмкіндік береді.	Тағайындалмаған	Барлық үдерістер үшін қосылған
ActiveX элементтерін орнату	Саясаттың бұл параметрі Internet Explorer процестері үшін ActiveX бақылауын	Тағайындалмаған	Барлық үдерістер үшін қосылған

шектеулері	орнату сұранысының бұғатталуын басқарады.		
Файлдарды жүктеу шектеулері	Саясаттың бұл параметрі қолданушы емес файлдарды жүктеуге арналған сұраныстардың бұғатталуын басқарады.	Тағайындалмаған	Барлық үдерістер үшін қосылған
Қондырмаларды басқару (Управление надстройками)	Бұл саясат сізге Internet Explorer қондырмаларының тізімінде көрсетілмеген барлық параметрлерден бас тартуға мүмкіндік береді.	Тағайындалмаған	«Қондырмалар тізімі» саясатымен бекітілмеген басқа барлық қондырмаларға бас тыйым салынған» параметрі қосылған
Желілік хаттаманы бұғаттау	Саясаттың бұл параметрі қауіпсіздік аймақтарының әрқайсысы үшін тыйым салынған хаттамалардың тізімін анықтайды	Тағайындалмаған	Әрбір қауіпсіздік аймақтары үшін «Шектеулі хаттамалар» параметрін қосу

Бақылау сұрақтары

1. Осы уақытта желіде отырған барлық тұтынушылардың тізімін қалай көруге болады?
2. Қашықтан байланыста отырып нөмір бойынша автоматты қоңырау шалуды қалай орнатуға болады?
3. Желілік дискіні қалай қосуға (жалғауға) болады?