ОЖҚ. Зертханалық жұмыс №8. ФИЗИКАЛЫҚ ОБЪЕКТІНІҢ КӨМЕГІМЕН ОПЕРАЦИЯЛЫҚ ЖҮЙЕЛЕРДЕ ЖҮРГІЗІЛЕТІН АУТЕНТИФИКАЦИЯ

Зертхананың мақсаты: физикалық нысан – eToken көмегімен операциялық жүйеде (ОЖ) аутентификацияға мүмкіндік беретін утилиталар мен қолданбаларды қарастыру.

Зертханалық жұмыстың міндеттері:
1. eToken көмегімен негізгі әрекеттер
2. eToken PIN коды үшін сапа талаптарын орнату
3. eToken әкімшілігі
4. eToken көмегімен ОЖ-да аутентификация
5. Кездейсоқ құпия сөзге негізделген ОЖ аутентификациясы
6. eTokenNetworkLogon тапсырмасын басқару

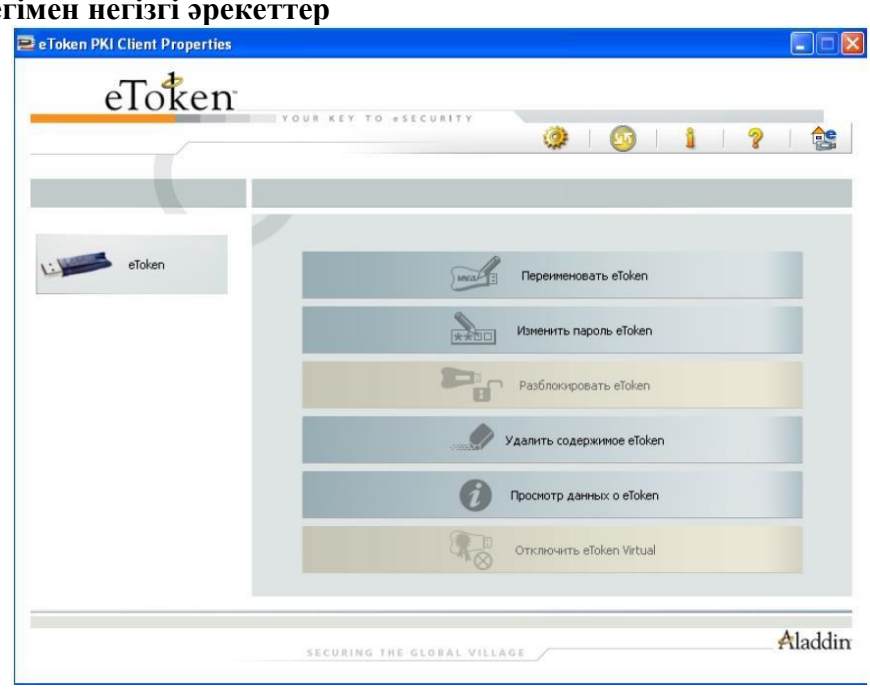
тест сұрақтары

Зертханалық жұмыстың мазмұны::

Зертханада операциялық жүйеге кіру құпия сөзі физикалық нысанда сақталады және оған eToken ішіндегі PIN коды арқылы қол жеткізіледі. eToken компьютерге қосу үшін USB порты пайдаланылады.

Қарастырылған утилиталар мен қосымшалар:
- *eToken басқару утилитасы – оған PIN-кодтың сапасын орнатуға мүмкіндік береді;*
- *eToken Network Logon - OS жүйесіне кіру үшін аутентификация деректерін сақтау үшін eToken пайдалануға мүмкіндік береді.*

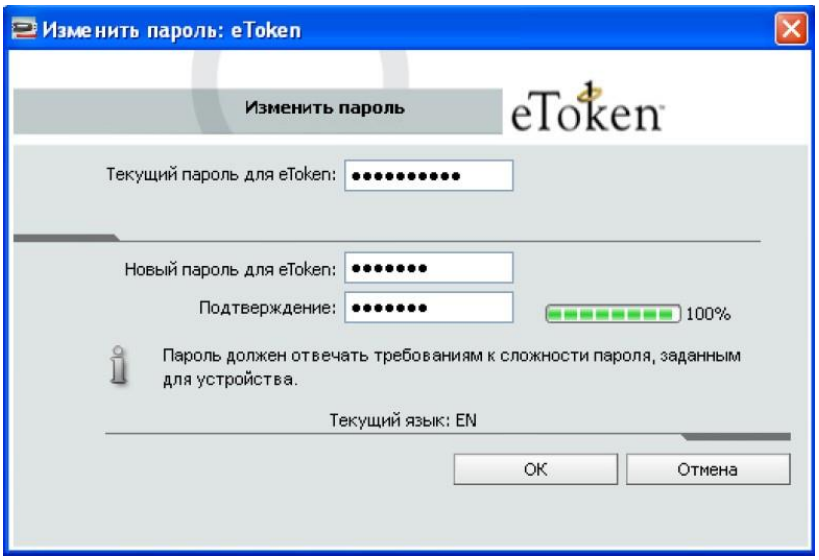
1. eToken көмегімен негізгі әрекеттер



Сурет 1 - "eToken Properties"қызметтік терезесінің негізгі көрінісі

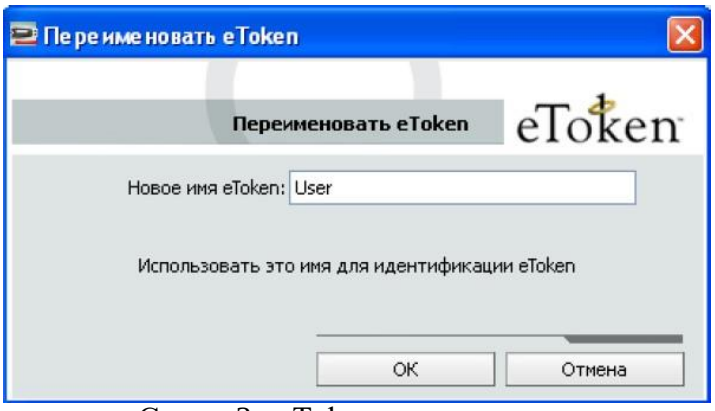
Виртуалды ОЖ іске қосыңыз және «Әкімші» тіркелгісімен кіріңіз. eToken құрылғысын USB портына қосыңыз. "eToken Properties" қызметтік бағдарламасын іске қосыңыз: "Бастау - Бағдарламалар - eToken - eToken сипаттары" (немесе хабарландыру жолағындағы "eToken PKI клиенті" белгішесі арқылы). Негізгі терезенің көрінісі күріште көрсетілген. бір.

Смените PIN-код. Используемый по умолчанию PIN-код: «1234567890». При сменеPIN-кода необходимо соблюдать требования, предъявляемые к его качеству. Достижение отметки 100% означает, что введённый PIN-код отвечает установленным требованиям (рис. 2).

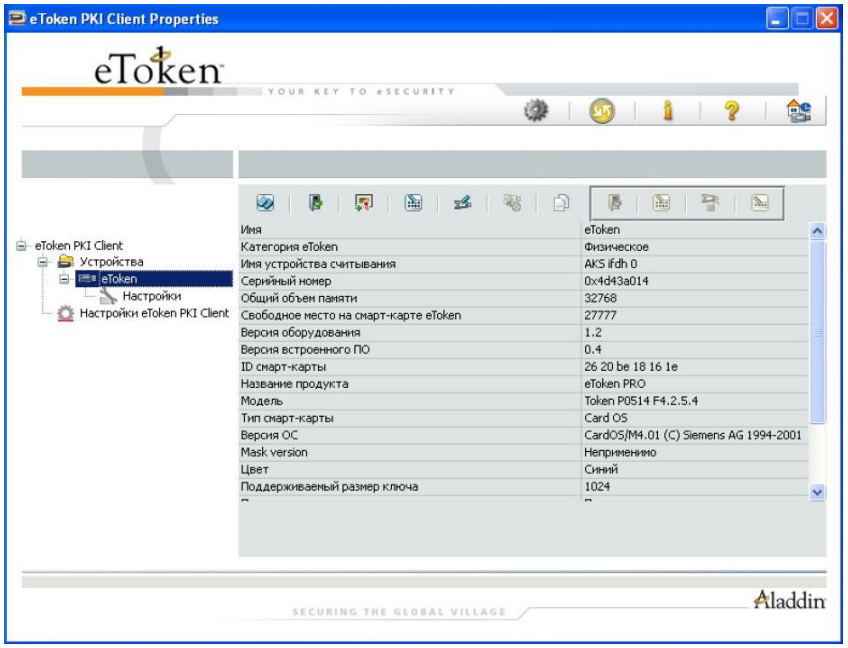


Сурет. 2 - PIN кодын өзгерту

eToken атауын өзгерту (3-сурет). eToken иелігін оңай анықтау үшін оған eToken берілген жүйеде бірегей пайдаланушы идентификаторын (логин) тағайындау қажет. eToken бірінші рет пайдаланған кезде, PIN кодын енгізу керек.
Интерфейс режимін «Егжей-тегжейлі қарау» күйіне өзгертіңіз (құралдар тақтасындағы белгіше). Бұл режим қосылған eTokens-пен жұмыс істеу үшін қосымша параметрлер мен функцияларға қол жеткізуді қамтамасыз етеді (Сурет 4). Негізгі режим терезесінде
"Толық көрініс" таңдалған eToken туралы ақпаратты береді.



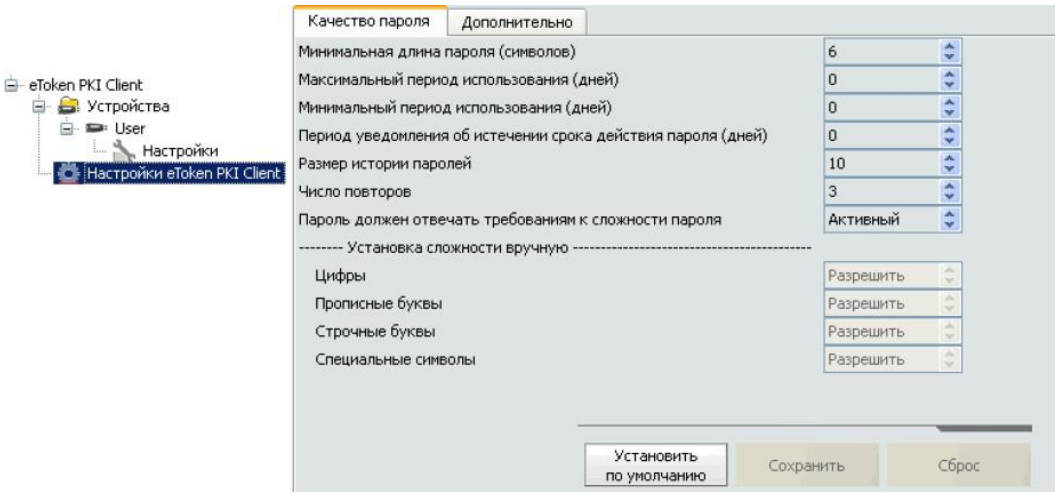
Сурет. 3 - eToken атауын өзгерту



Сурет. 4 - «Егжей-тегжейлі қарау» режимінде eToken үшін негізгі терезенің көрінісі

1. eToken PIN коды үшін сапа талаптарын орнату

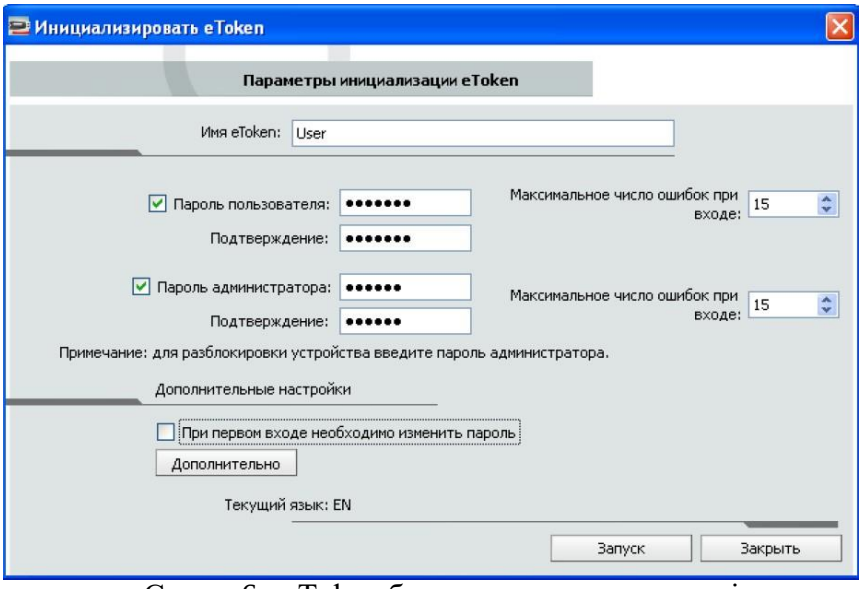
«eToken PKI Client Settings» бөлімінде пішімдеу кезінде оған жазылатын eToken PIN кодының сапасына қойылатын талаптарды орнатуға болады (5-сурет). eToken-де сақталған талаптарды қарау таңдалған eToken-тің "Параметрлер" бөлімінде мүмкін болады.



Сурет. 5 - eToken PIN сапа параметрлерін орнату

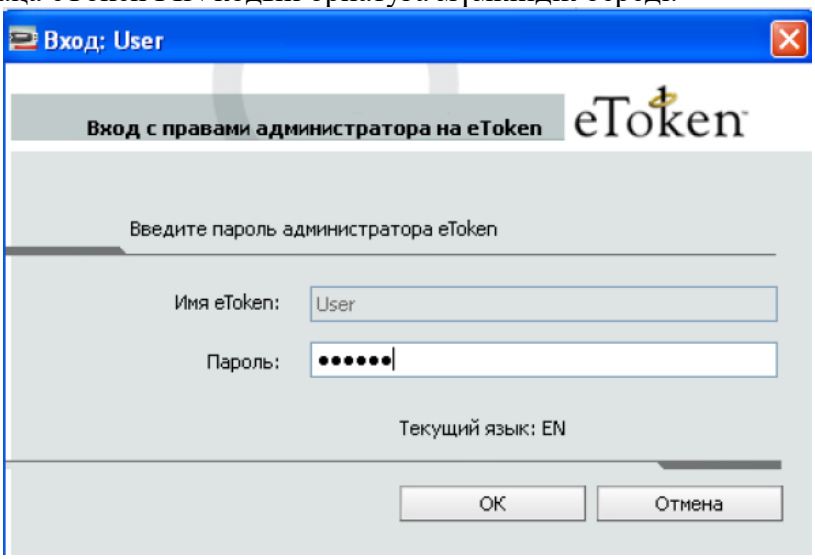
1. eToken әкімшілігі

Егжей-тегжейлі көрініс қосылған eToken таңдаңыз және құралдар тақтасынан eToken инициализациясын таңдаңыз. eToken Initialization Settings терезесінде (6-сурет) eToken PIN кодын немесе бірінші рет пайдаланған кезде құпия сөзді өзгерту талабын (егер сіз әдепкі PIN кодын қалдырсаңыз) және eToken әкімшісінің PIN кодын орнатыңыз. Сондай-ақ, сәйкес PIN кодтарын және eToken атауын енгізу кезіндегі қателердің ең көп санын орнатуға болады. eToken пішімі. Назар аударыңыз! Пішімдеу кезінде пішімдеу кілтін көрсетуге болады («Қосымша»
- «Бастау кілтін өзгерту»). Бұл қойындының параметрлерін өзгертпеңіз, өйткені пішімдеу кілтін білмесеңіз, оны бастапқы күйіне қайтара алмайсыз, бұл eToken жұмыс істемеуіне әкеледі.



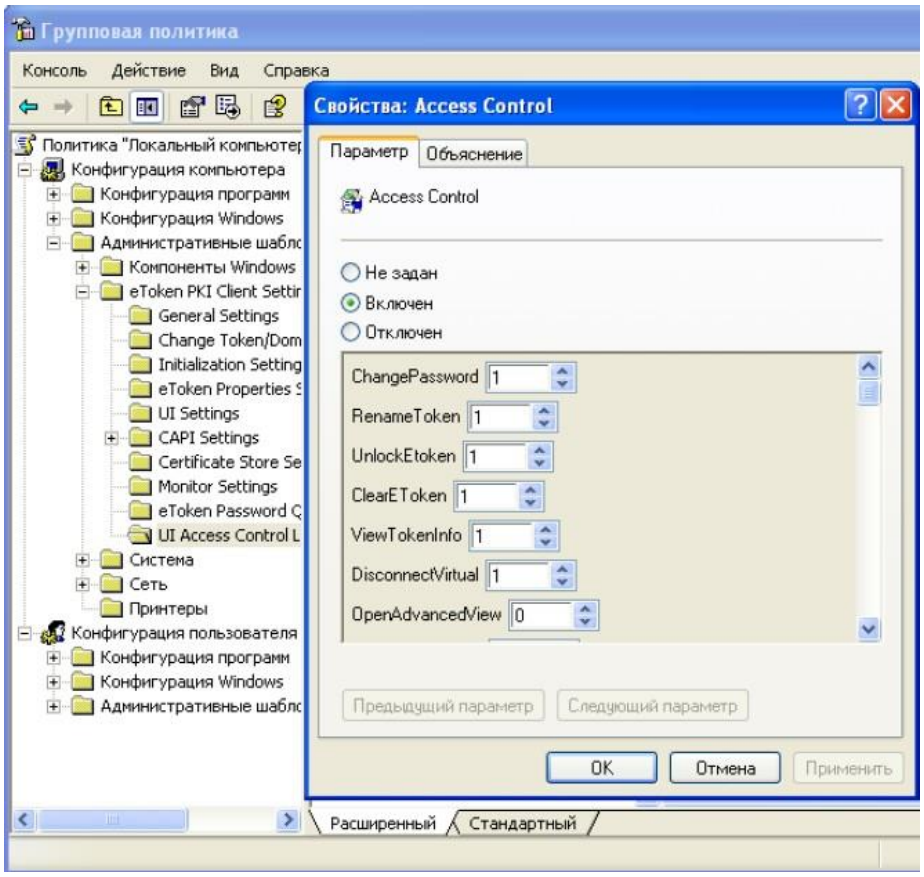
Сурет. 6 - eToken баптандыру параметрлері

Қосылған eToken таңдаңыз. Құралдар тақтасынан Әкімшіге кіру белгішесін таңдаңыз. Әкімшінің PIN кодын енгізіңіз (сур. 7). Әкімші қосымша функциялармен қамтамасыз етілген. Құралдар тақтасында белгішені таңдаңыз
«Пайдаланушы құпия сөзін орнату». Бұл мүмкіндік пайдаланушы ағымдағы PIN кодын ұмытып қалса, әкімшіге жаңа eToken PIN кодын орнатуға мүмкіндік береді.



Сурет. 7 - Әкімші құпия сөзін енгізу

"eToken Properties" қызметтік бағдарламасының интерфейс параметрлерін тиісті әкімшілік үлгіні пайдаланып "Топтық саясаттар" арқылы өзгертуге болады. gpedit.msc қосымша модулін ашыңыз және eTokenPKIClient.adm әкімшілік үлгісін қосыңыз (жұмыс үстелінде орналасқан). Пайда болған «eToken PKI Client Settings» бөлімінде қарастырылып отырған утилитаның кез келген параметріне кіруге рұқсат беруге немесе тыйым салуға болады. Мысалы, «Егжей-тегжейлі көрініс» режиміне кіруді өшіріңіз («UI қатынасын басқару тізімі» бөлімінің «Access Control» параметрінің «OpenAdvancedView» параметрінің 0 мәні, 8-сурет). Жасалған өзгерістерді тексеру үшін eToken Properties утилитасын қайта іске қосыңыз.



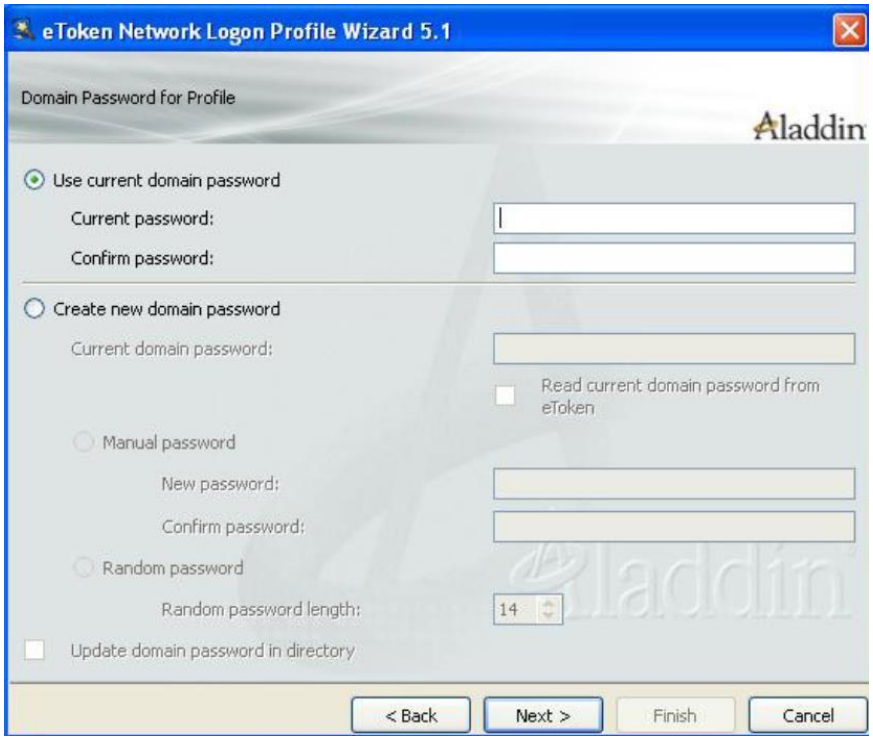
Сурет. 8 - «Жетілдірілген» режимге кіруге тыйым салу

1. eToken көмегімен ОЖ-да аутентификация

Операциялық жүйеге кіру профилін жасау үшін қызметтік бағдарламаны іске қосыңыз: «Бастау - Бағдарламалар - eToken - eToken желіге кіру - eToken желіге кіру профилінің шебері». Келесі түймесін басыңыз. Пайдаланушы логинін (мысалы, «Пайдаланушы») және профиль жасалып жатқан жұмыс станциясының (немесе доменнің) атын енгізіңіз (Сурет 9). Келесі түймесін басыңыз.

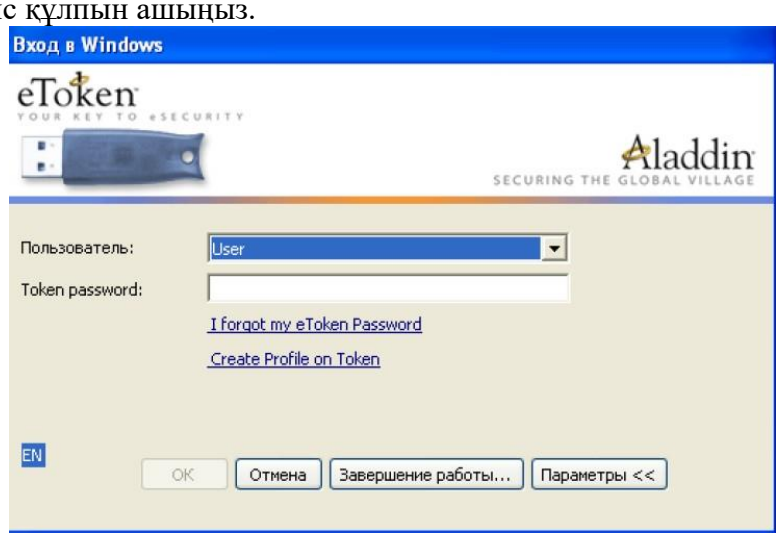
Сурет. 9 - ОЖ жүйесіне кіру үшін пайдаланушы ақпаратын енгізу

Таңдалған пайдаланушыға тиесілі ОЖ кіру құпия сөзін енгізіңіз және растаңыз (Сурет 10). «Келесі» түймесін екі рет басыңыз. Жасалған профиль оған жазылғанын растау үшін eToken PIN кодын енгізіңіз.



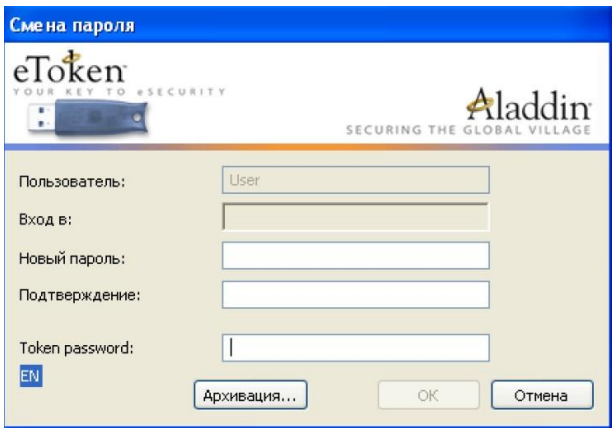
Сурет. 10 - Операциялық жүйеге кіру үшін құпия сөзді енгізу

Ағымдағы пайдаланушы сеансын аяқтаңыз және eToken өшіріңіз. Windows сәлемдесу терезесі пайда болған кезде eToken қосыңыз. Суретте көрсетілген терезе. 11. eToken PIN кодын енгізіп, OK түймесін басыңыз. Қажетті аутентификация ақпараты eToken-тен оқылады және ОЖ жүйеге кіреді. ОЖ-ге кіргеннен кейін eToken-ді өшіріңіз - бұл жағдайда пайдаланушы сеансы бұғатталған. eToken қосыңыз және сеанс құлпын ашыңыз.



Сурет. 11 - eToken көмегімен екі факторлы аутентификация

ОЖ-ға кіріктірілген құралдарды пайдаланып ОЖ-ға кіру құпия сөзін өзгертуге болады. Ctrl-Alt-Del пернесін басып, «Құпия сөзді өзгерту...» таңдаңыз. Пайда болған терезеде (12-сурет) жаңа құпия сөз мен оны растаудан басқа, оған жаңа құпия сөз жазу үшін eToken PIN кодын енгізу керек..



Сурет. 12 - Операциялық жүйеге кіру үшін құпия сөзді өзгерту

Сондай-ақ eToken желіге кіру профилі шебері утилитасын пайдаланып құпия сөзді өзгертуге болады. Терезеде (13-сурет) бар eToken профилін таңдаңыз. Терезеде (14-сурет) жаңа құпия сөзді жасауды таңдап, ОЖ қоймасында құпия сөзді жаңарту опциясын қосыңыз («Каталогтағы домен құпия сөзін жаңарту»). Ағымдағы және жаңа құпия сөздерді енгізіңіз. Ағымдағы құпия сөз eToken ішінде әлдеқашан болса, "eToken-тен ағымдағы домен құпия сөзін оқу" параметрін қосыңыз және қызметтік бағдарлама оны бұрыннан бар профильден автоматты түрде оқиды.

Сурет. 13 - Бар eToken профилін таңдау

Сурет. 14 - Операциялық жүйеге кіру үшін құпия сөзді өзгертіңіз

eToken-те бар профильді жою үшін терезеде таңдау керек (Сурет 15)
«Бар профильді жою». Бар профильді жою.

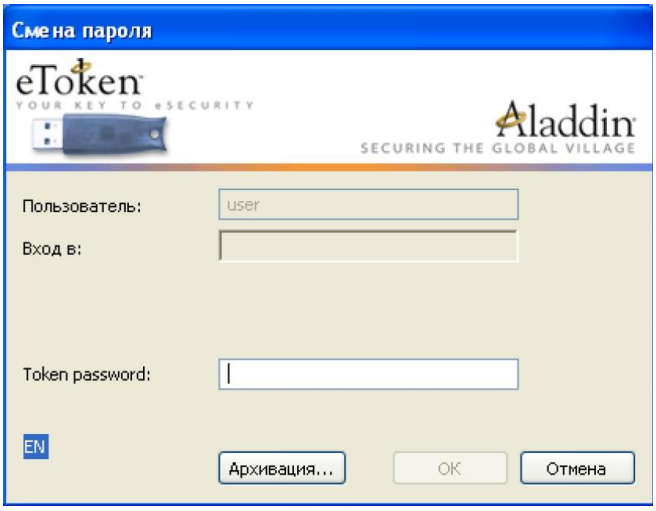
Сурет. 15 - Екі факторлы аутентификацияны таңдау

2. Кездейсоқ құпия сөзге негізделген ОЖ аутентификациясы

Белгілі бір ұзындықтағы кездейсоқ құпия сөзді орнатуды таңдау арқылы ОЖ жүйесіне кіру үшін жаңа профиль жасаңыз (Сурет 16). Содан кейін ОЖ-ға кіру құпия сөзі тек eToken-де сақталады, күрделілігі жоғары, пайдаланушыға белгісіз болады, бұл парольді болжау немесе ашу мүмкіндігін азайтады. Профиль жасағаннан кейін пайдаланушы сеансын аяқтаңыз. eToken өшіру. ОЖ-ға стандартты кіру әрекеті кезінде (Ctrl-Alt-Del арқылы) ескі пайдаланушы құпия сөзі қабылданбайды, себебі. құпия сөз белгіленген ұзындықтағы кездейсоқ біреуге өзгертілді. eToken арқылы ОЖ жүйесіне кіріңіз.

Сурет. 16 - Операциялық жүйеге кіру үшін кездейсоқ құпия сөзді орнату

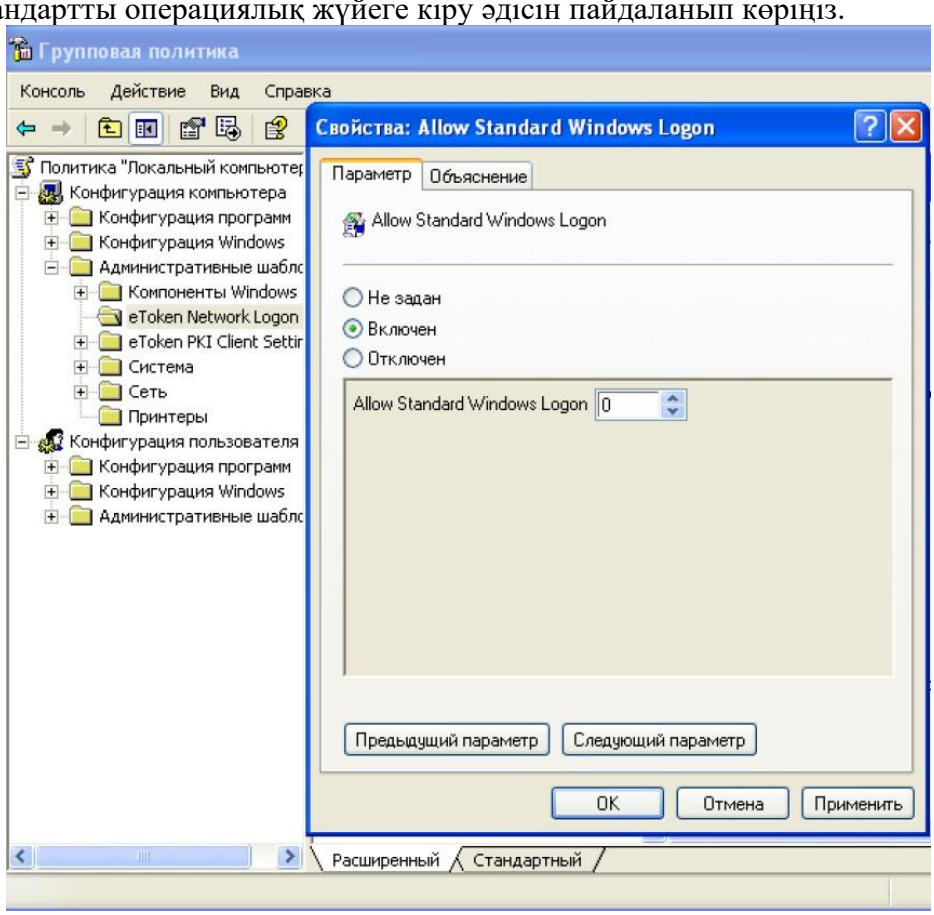
Пайдаланушы Ctrl-Alt-Del пернесін басқан кезде «Парольді өзгерту ...» таңдау арқылы ОЖ-ға кіру үшін кездейсоқ құпия сөзді өзгерте алады (Сурет 17). Бұл жағдайда eToken PIN кодын енгізу жеткілікті, ал ОЖ енгізу үшін жаңа құпия сөз кездейсоқ түрде жасалады. Кездейсоқ құпия сөздің ұзындығы параметрлерге сәйкес орнатылады.



Сурет. 17 - Операциялық жүйеге кіру үшін кездейсоқ орнатылған құпия сөзді өзгерту

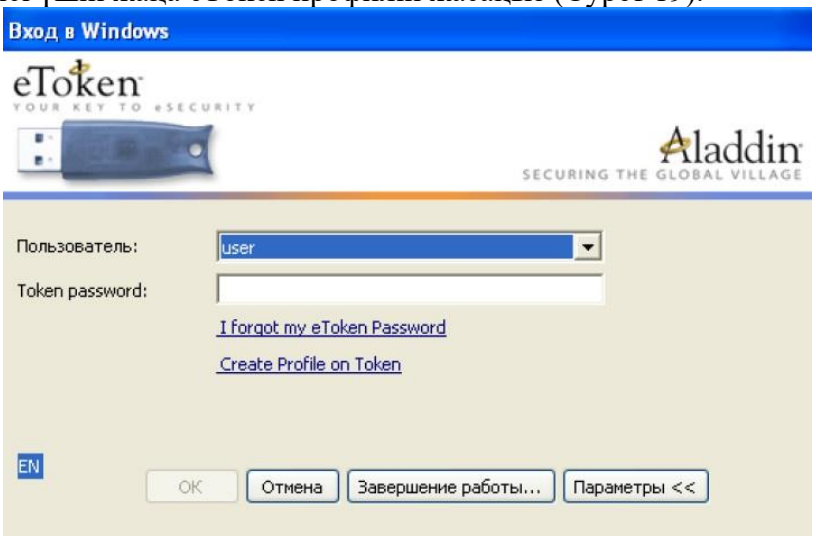
3. eTokenNetworkLogon әкімшілігі

Қарастырылып отырған қызметтік бағдарламаның параметрлерін тиісті әкімшілік үлгіні пайдаланып «Топтық саясаттар» арқылы өзгертуге болады. Әкімші тіркелгісі астында gpedit.msc ашыңыз, әкімшілік үлгіні қосыңыз
"C:\Program Files\Aladdin\eToken\eTNLogon\eTokenNetworkLogon.adm". тарауда
"eTokenNetworkLogon" кез келген параметрге кіруге рұқсат беруге немесе тыйым салуға, сондай-ақ қарастырылып отырған утилитаның функцияларын қосуға немесе өшіруге болады. Мысалы, Ctrl-Alt-Del арқылы ОЖ-ға стандартты кіруді өшіріңіз («Windows стандартты кіруіне рұқсат беру» параметрі үшін 0 мәні) - кіруге eToken арқылы ғана рұқсат етіледі (Сурет 18). Пайдаланушы сеансын аяқтаңыз. Стандартты операциялық жүйеге кіру әдісін пайдаланып көріңіз.



Сурет. 18 - ОЖ-ға стандартты кіруге тыйым салу

Әкімші құқықтарымен жүйеге кіру үшін «Токенде профиль жасау» функциясын пайдаланып, «Әкімші» тіркелгісі үшін жаңа eToken профилін жасаңыз (Сурет 19).



Сурет. 19 - eToken-пен жұмыс істеуге арналған функциялар операциялық жүйеге кірер алдында қолжетімді

Жаттығу

1. Собор желісінде атыңыздың атымен бірдей пайдаланушы жасаңыз.
2. Өз опцияңызға сәйкес eToken PIN-кодының сапасына қойылатын талаптарды орнатыңыз (1-кесте).
3. eToken-ті оған жасалған пайдаланушының атын беру және 2-тармақтың талаптарына сәйкес келетін құпия сөзді орнату арқылы пішімдеңіз.
4. Жасалған пайдаланушының ОЖ жүйесіне кіру үшін профиль жасаңыз.
5. Оқытушыға нұсқаңызда көрсетілген параметрлерге сәйкес ОЖ-ға кіру паролін өзгерту тәртібін көрсетіңіз.

Кесте 1. Тапсырма опциялары

Вар.	***PIN код сапасына қойылатын талаптар***	***ОЖ жүйесіне кіру опциялары***
1	Мин. пароль ұзындығы - 8 таңба. Макс. пароль 30 күн бойы жарамды.	Жаңа құпия сөзді қолмен енгізу. Ағымдағы құпия сөзді қолмен енгізу.
2	Мин. пароль ұзындығы - 12 таңба. Соңғы сақталған құпия сөздердің саны - 5.	Жаңа құпия сөзді қолмен енгізу Ағымдағы құпия сөзді мына жерден оқу eToken.
3	Мин. пароль ұзындығы - 12 таңба. Құпия сөз тек екі жағдайдың да әріптерін қамтуы керек.	Жаңа құпия сөзді қолмен енгізу Ағымдағы құпия сөзді мына жерден оқу eToken.
4	Макс. пароль 30 күн бойы жарамды. Құпия сөз таңбалардың барлық түрлерін қамтуы керек.	Ұзындығы 10 таңбадан тұратын кездейсоқ жаңа құпия сөзд жасаңыз. Ағымдағы құпия сөзді қолмен енгізу.
5	Макс. пароль 40 күн бойы жарамды. Соңғы сақталған құпия сөздердің саны - 8.	Ұзындығы 10 таңбадан тұратын кездейсоқ жаңа құпия сөзд жасаңыз. eToken қолданбасынан ағымдағы

		құпия сөзді оқу.
6	Мин. пароль ұзындығы - 10 таңба. Құпия сөз тек регистрлер мен сандардан тұратын әріптерден тұруы керек.	Генерация случайного нового пароля длиной 10 символов.

		Ағымдағы құпия сөзді қолмен енгізу.
7	Мин. пароль ұзындығы - 12 таңба. Құпия сөз таңбалардың барлық түрлерін қамтуы мүмкін.	Кездейсоқ жаңа генерация 15 таңбадан тұратын құпия сөз Ағымдағы құпия сөзді қолмен енгізу.
8	Макс. пароль 30 күн бойы жарамды. Пайдаланушыға парольді өзгерту туралы қанша күнде ескерту керек - 3 күн.	15 таңбадан тұратын кездейсоқ жаңа құпия сөзді жасаңыз Ағымдағы құпия сөзді мына жерден оқу eToken.
9	Соңғы сақталған құпия сөздердің саны - 7. Құпия сөз тек регистрлер мен сандардан тұратын әріптерден тұруы керек.	Ctrl-Alt-Del арқылы құпия сөзд өзгертіңіз.
10	Соңғы сақталған құпия сөздердің саны - 9. Құпия сөз таңбалардың барлық түрлерін қамтуы керек.	Кездейсоқты өзгерту Ctrl-Alt-Del арқылы құпия сөз.

Тест сұрақтары

1. Әдепкі eToken PIN коды дегеніміз не?
2. eToken-тегі бос жад көлемін қалай білуге болады?
3. eToken әкімшісіне қандай қосымша опциялар қолжетімді?
4. eToken PIN кодына қандай сапа талаптарын қоюға болады?
5. Осы PIN кодын өзгерту кезінде пайдаланылатын eToken PIN сапасына қойылатын талаптар қайда сақталады?
6. eToken көмегімен екі факторлы аутентификация мен бір факторлы аутентификация арасындағы айырмашылықтарды сипаттаңыз.
7. eToken Network Logon қолданбасы арқылы жасалған кіру профилі нені қамтиды?
8. Операциялық жүйеге кіру үшін пайдаланушының құпия сөзін өзгертудің қандай әдістерін қолдануға болады?
9. Пайдаланушы операциялық жүйеге кіру үшін кездейсоқ орнатылған парольді қалай өзгертеді?
10. Әр түрлі eToken сипаттарының және eToken желіге кіру мүмкіндіктерінің пайдаланушы қол жетімділігі қалай конфигурацияланады?

Жаттығу

Зертханалық есеп нұсқаулықта сипатталған стандартқа сәйкес орындалады

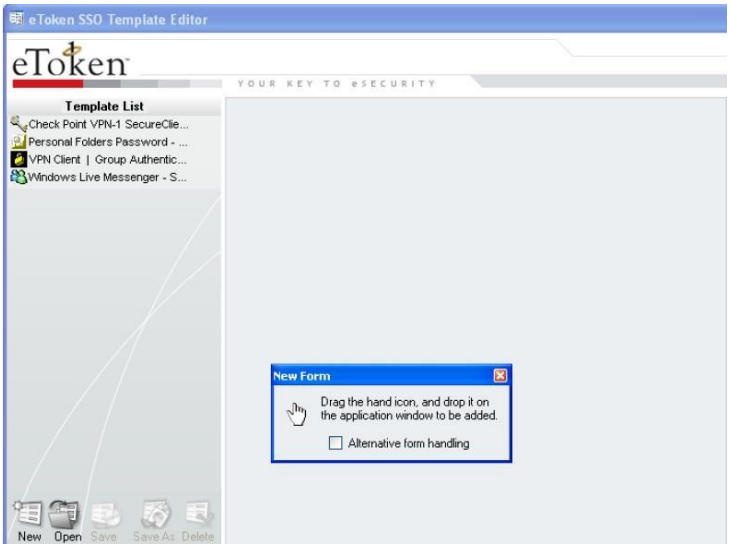
ОЖҚ. Зертханалық жұмыс №9. БАҒДАРЛАМАЛЫҚ ЖАСАҚТАМАДА SSO ТЕХНОЛОГИЯСЫНА НЕГІЗДЕЛГЕН ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯ ЖҮРГІЗУ

Зертханалық жұмыстың мақсаты: қолданбалы қосымшаларда және веб-сайттарда аутентификация жасауға мүмкіндік беретін утилиталарды физикалық нысан - eToken көмегімен қарастыру.

Зертханалық жұмыстың міндеттері:
1. Қолданбаның аутентификация терезесінің үлгісін жасау
2. Қолданбаның аутентификация деректерімен eToken - де профиль жасау
3. Веб-сайттардағы екі факторлы аутентификация
4. EToken SSO тапсырмасын басқару
Бақылау сұрақтары

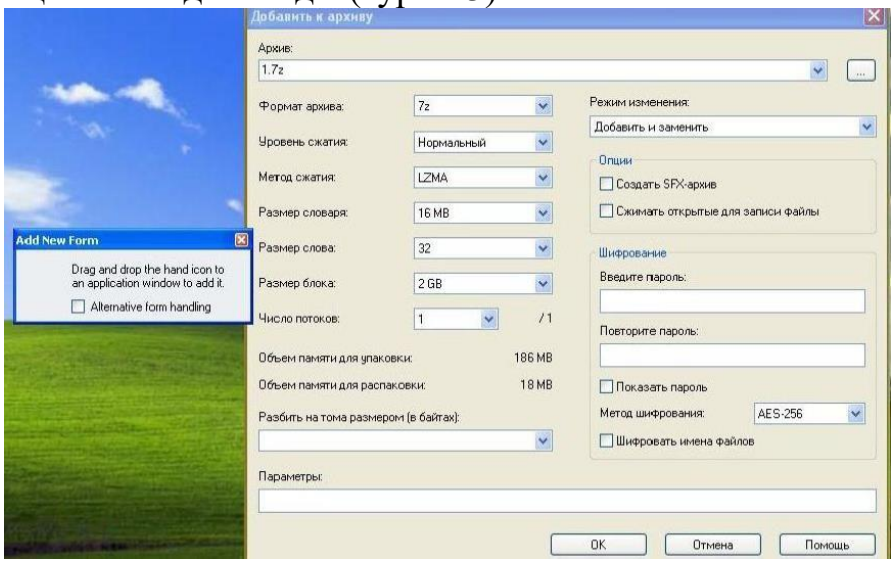
Зертханалық жұмыстың мазмұны:
Бұл зертханалық жұмыста утилиталар қарастырылады:
- eToken SSO Template Editor - аутентификация деректерін енгізу өрістерін қамтуы мүмкін әр түрлі қосымшалар мен веб-сайттардың терезе шаблондарын жасауға мүмкіндік береді (тек әкімші компьютерінде орнатылған);
- eToken SSO Client-әр түрлі қосымшалардың аутентификация деректерін сақтау үшін eToken-ді пайдалануға және осы деректерді тиісті қолданба терезелеріне енгізуге мүмкіндік береді (әр жұмыс станциясына орнатылған).

1. Қолданбаның аутентификация терезесінің үлгісін жасау
Қолданбалар мен веб - сайттар үшін деректерді енгізу үлгісін басқару утилитасын іске қосыңыз: "бастау - бағдарламалар - eToken - eToken SSO - Template Editor". Құпия сөзбен қорғалған мұрағаттың "7-Zip" қосымшасын пайдаланып қалыптастыру үшін шаблон жасаңыз. Ерікті файлдың мәтінмәндік мәзірінен "7-Zip" - "мұрағатқа қосу"тармағын таңдаңыз.
Утилита терезесінің төменгі жолағында шаблон жасау үшін "жаңа" батырмасын басыңыз (сурет. 1).

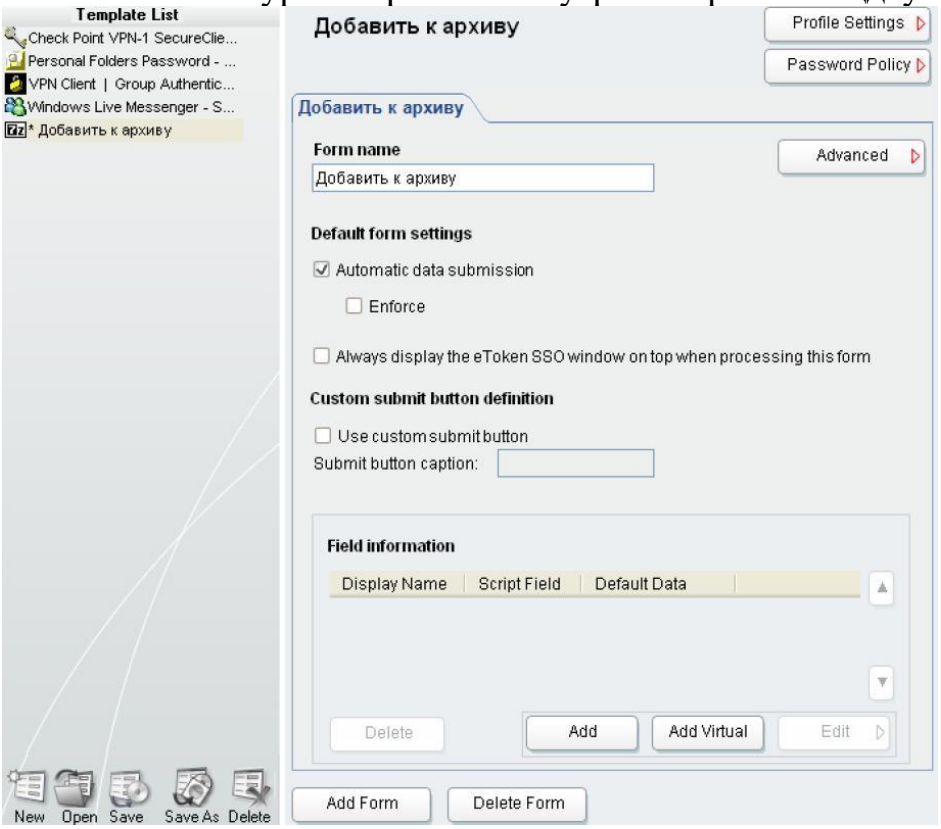


Сурет. 1 - "eToken SSO Template Editor"утилитасының негізгі терезесі

Содан кейін суреттегі алақанды "7-Zip" терезесіне сүйреңіз (сурет. 2). Бұл жағдайда шаблон өңдеуге қол жетімді болады (сурет. 3).

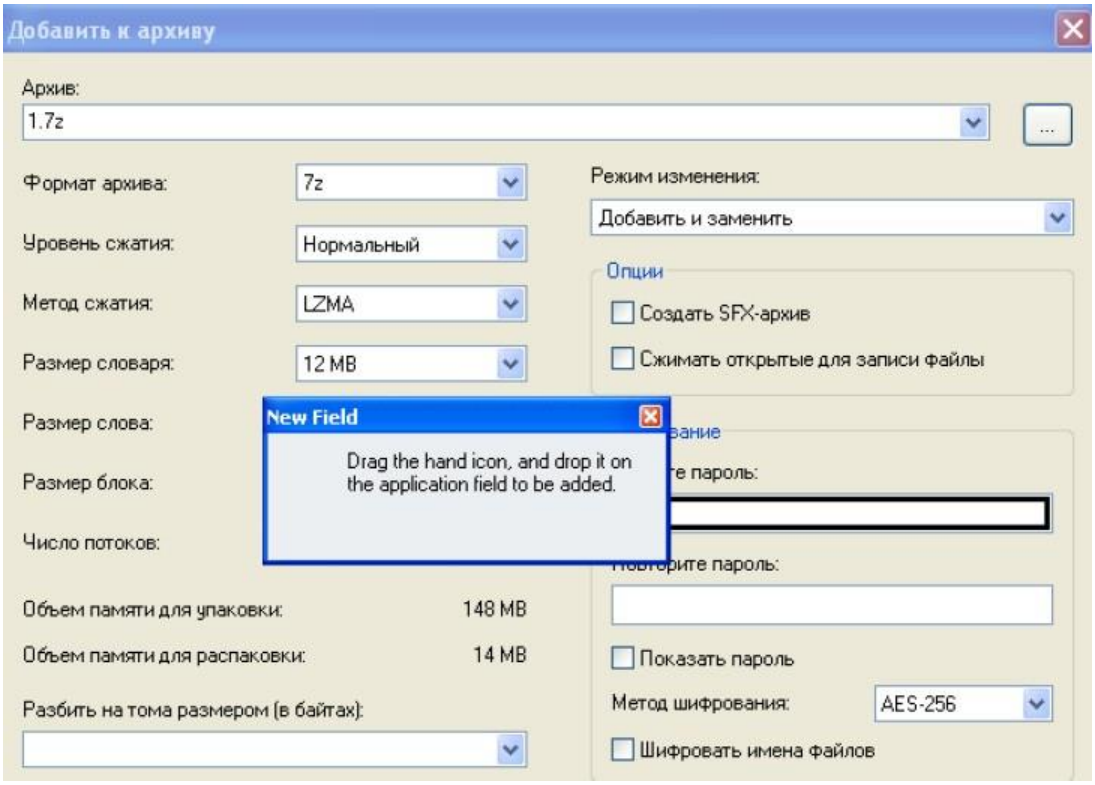


Сурет. 2-үлгіні жасау үшін терезені таңдау



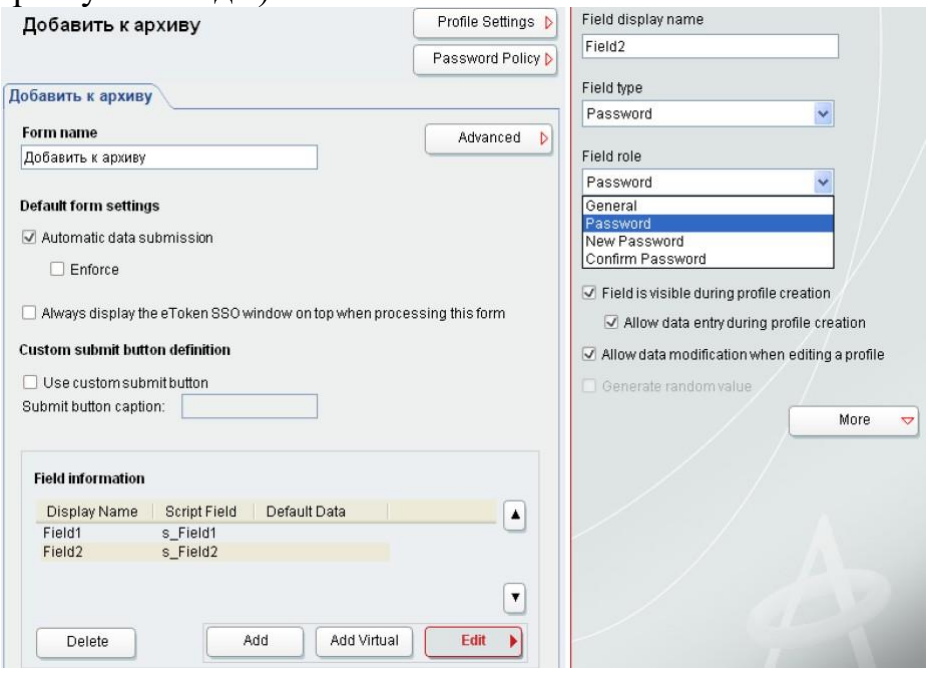
Сурет. 3-таңдалған қолданба терезесі үшін үлгі параметрлері

Терезедегі деректерді енгізу өрістері түймені басу арқылы қосылады
"Қосу" және пайда болған алақанды сүйреп апарыңыз. Өрістерді қосыңыз: "құпия сөзді енгізіңіз" (сурет.4) және "құпия сөзді қайталаңыз".



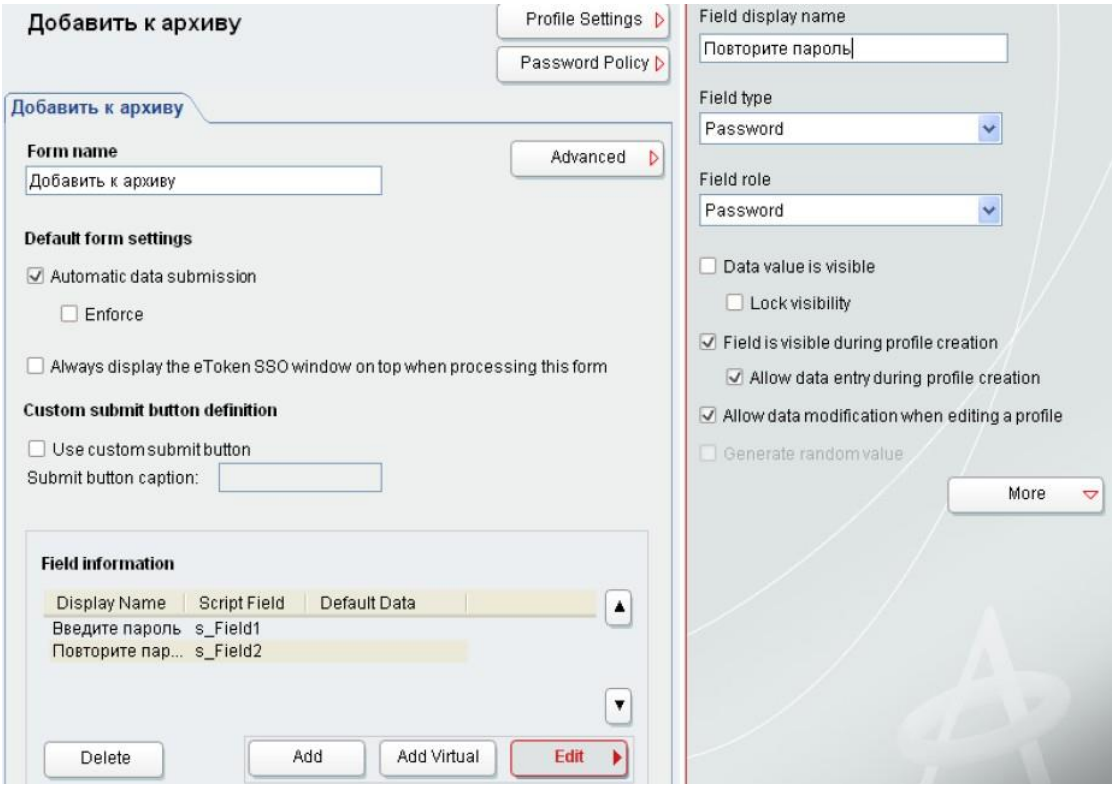
Сурет. 4 - "құпия сөзді енгізу"өрісін таңдау

Бұл жағдайда "құпия сөзді қайталаңыз " өрісі үшін өрістің" рөлін ""генералдан" өзгертіңіз
"Пароль" (сурет. 5), бұл өріске енгізілген таңбаларды жұлдызша түрінде көрсетуге мүмкіндік береді (тиісті өріс үшін "Өңдеу" батырмасын басу арқылы параметрлердің деректерін көрсетуге болады).



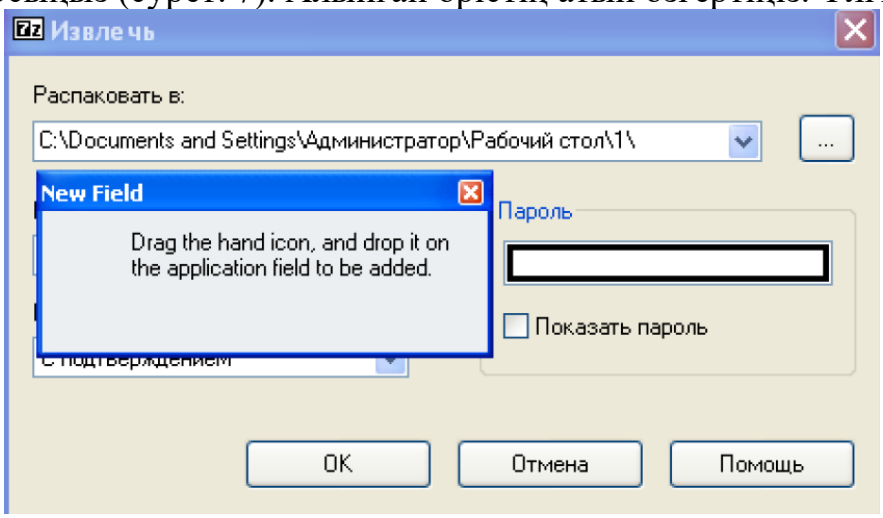
Сурет. 5-өрістің "рөлін" өзгерту

Үлгіні пайдалануды жеңілдету үшін қосылған Fieldi және Field2 өрістерінің атын ("Field display name") өзгертіңіз (сурет. 6). Негізгі терезенің төменгі жағындағы "Сақтау" түймесін басу арқылы үлгіні сақтаңыз.



Сурет. 6-үлгінің атын өзгерту

Құпия сөзбен қорғалған мұрағаттан файлдарды шығару үшін үлгі жасаңыз. Мұрағаттың мәтінмәндік мәзірінен "7-Zip" - "ашу"тармағын таңдаңыз. Үлгіге пароль енгізу өрісін қосыңыз (сурет. 7). Алынған өрістің атын өзгертіңіз. Үлгіні сақтаңыз.



Сурет. 7-файлдарды шығару терезесі үшін "құпия сөз" өрісін таңдау

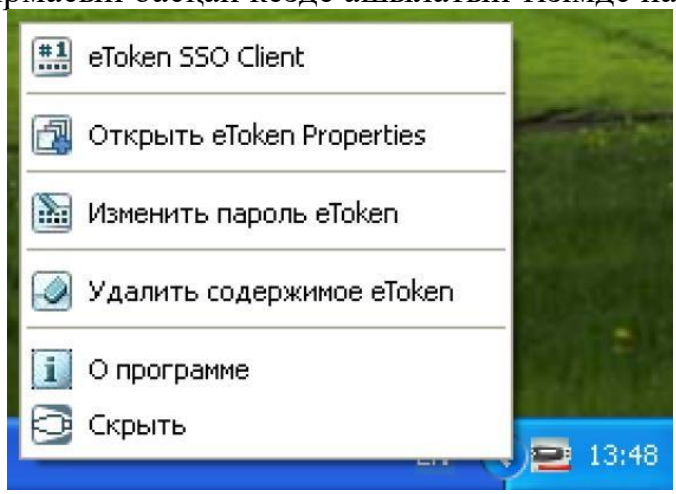
2. Қолданбаның аутентификация деректерімен eToken - де профиль жасау

Әдепкі бойынша, шаблондар "Менің құжаттарым\u003d SSO Templates" каталогына сақталады. Компьютердегі пайдаланушылар шаблондармен жұмыс істей алатындай етіп, бұл шаблондарды пайдаланушы профиліндегі "Менің құжаттарым\SSO client Templates" каталогына көшіру керек.

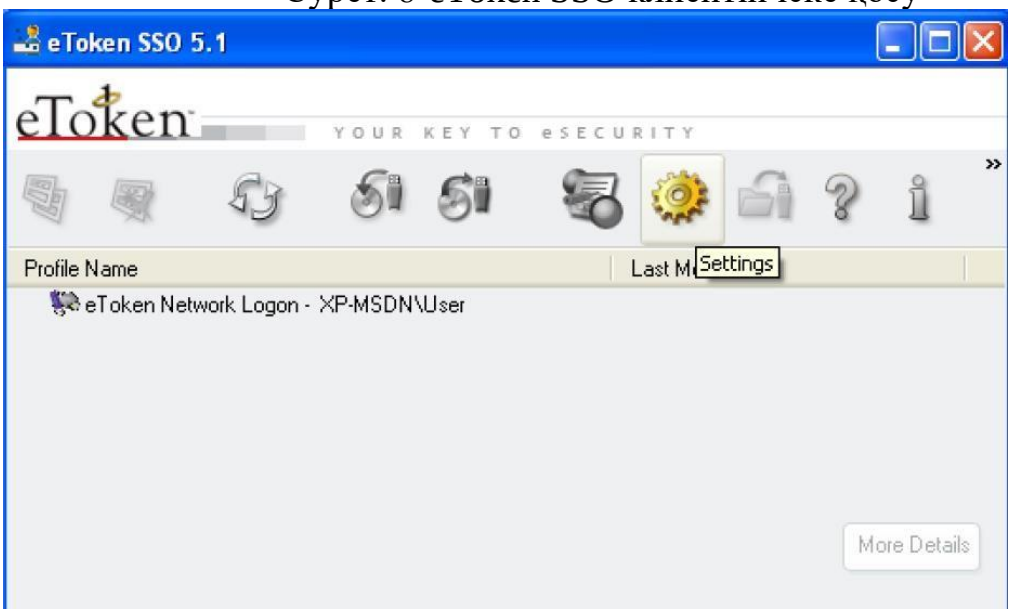
EToken SSO клиентін ашыңыз (сурет. 8). Құралдар тақтасында жаңарту түймесін басыңыз ("refresh Profile List"). Содан кейін eToken SSO Client параметрлерін ашыңыз

(сурет. 9). Егер

жасалған шаблондарды eToken SSO Client дұрыс жүктейді, содан кейін олар "show Loaded Templates"батырмасын басқан кезде ашылатын тізімде пайда болуы керек.

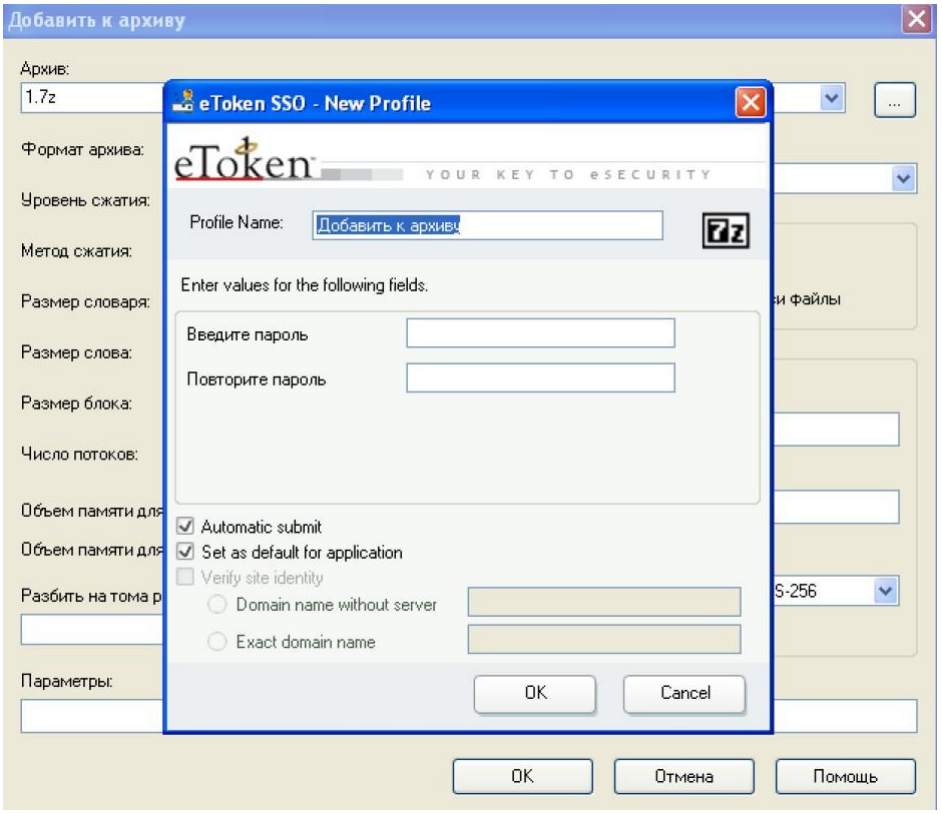


Сурет. 8-eToken SSO клиентін іске қосу



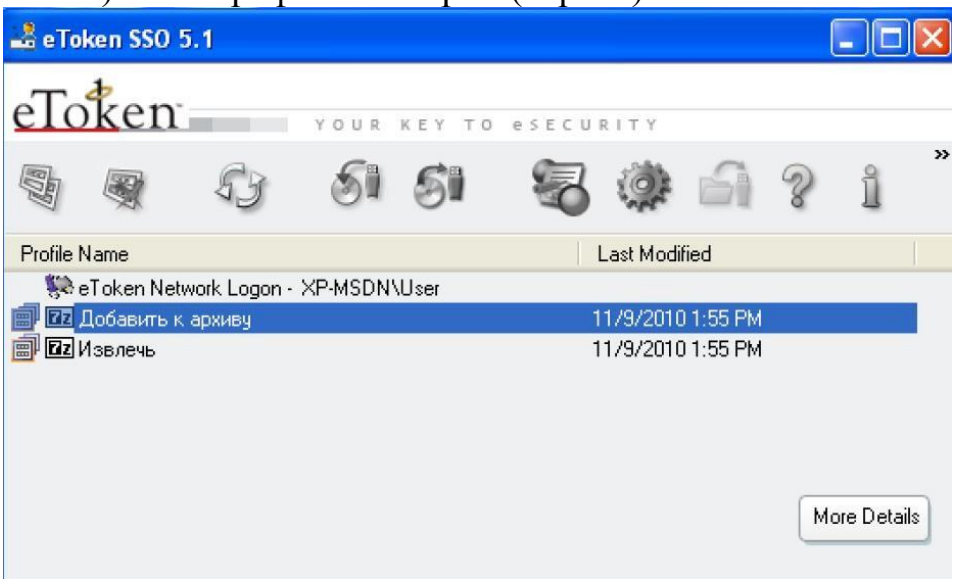
Сурет. 9 - "eToken SSO Client" утилитасының негізгі терезесінің көрінісі

Ерікті файл үшін "мұрағатқа қосу" терезесін ашыңыз. Шаблонға қолдау көрсетілетін терезені бірінші рет іске қосқан кезде, осы шаблонның өрістеріне арналған деректермен eToken-де профиль жасау ұсынылады (сурет. 10). Профиль жасау терезесіне мұрағаттау үшін құпия сөзді және оны Растауды енгізіңіз. Файлдарды ашу үшін бірдей әрекеттерді орындаңыз. Осылайша, файлдарды мұрағаттау / шығару кезінде eToken-де сақталған профильден пароль автоматты түрде енгізіледі. Ерікті файлды сынақтан өткізіңіз/шығарыңыз.

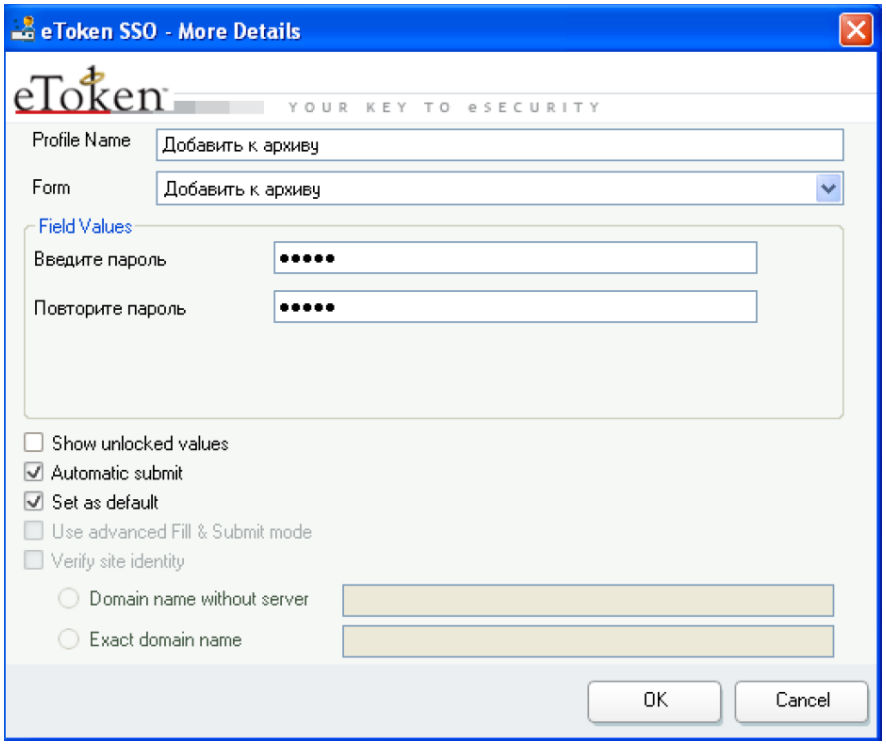


Сурет. 10-қолданба терезесі үшін eToken - де профиль жасау

Жасалған профильдер eToken SSO Client утилитасының негізгі терезесінде көрсетіледі (сурет. 11). Осы утилитаның көмегімен eToken-де сақталған профильдерді өңдеуге және жоюға болады. "7-Zip" үшін жасалған профильдердің бірін таңдап, Таңдалған профиль параметрлері терезесін көрсету үшін "толығырақ мәліметтер" түймесін басыңыз (сурет. 12). Бұл терезеде сіз таңдалған профильдің параметрлерін өзгерте аласыз (мысалы, OK батырмасын автоматты түрде басу - "Автоматты субмит") және профиль мазмұны (пароль).



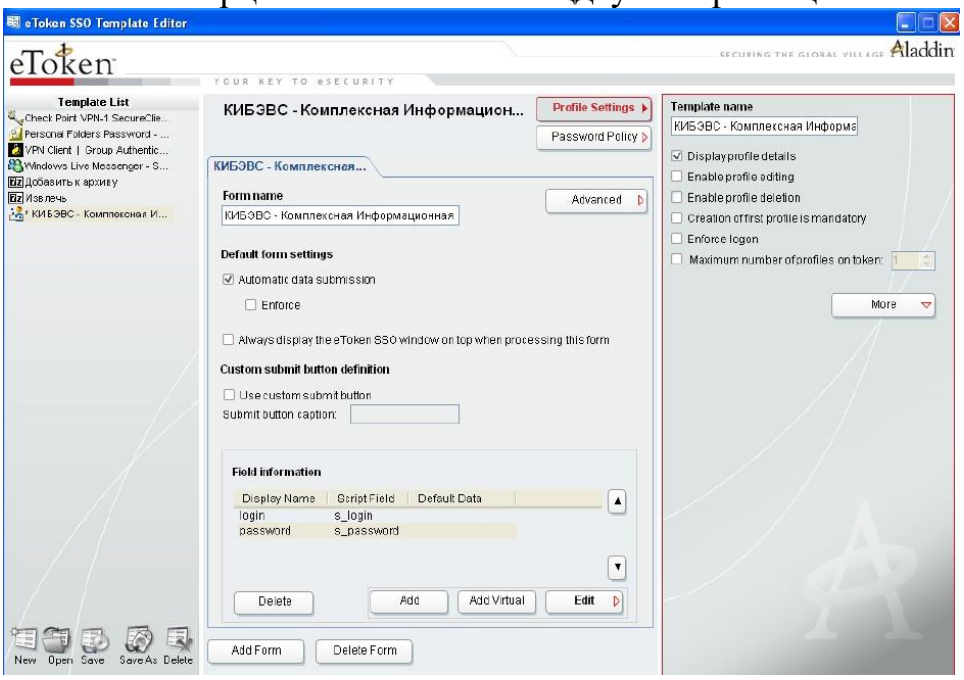
Сурет. 11-eToken - де сақталған Профильдер тізімі



Сурет. 12-Профильді және оның параметрлерін өңдеу

3. Веб-сайттардағы екі факторлы аутентификация

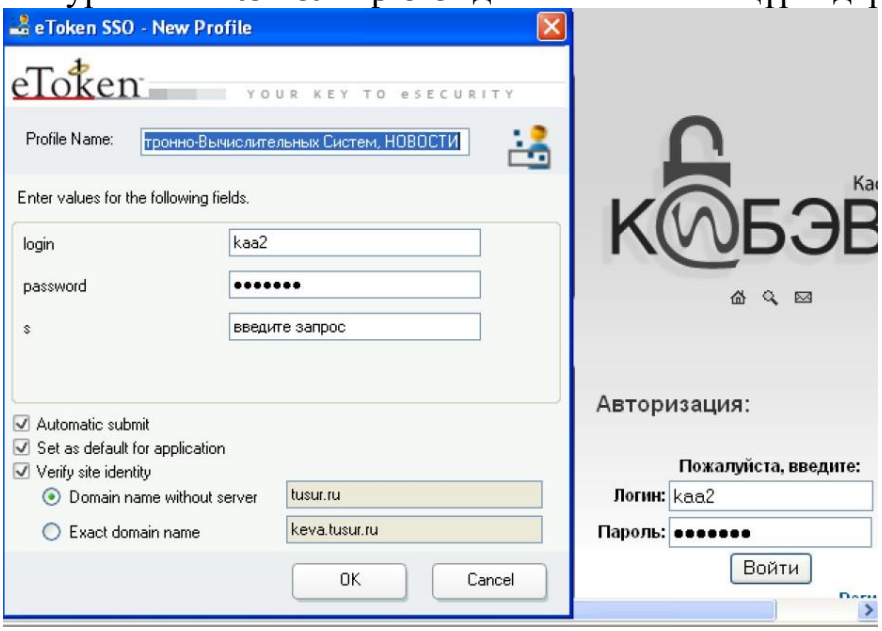
Қолданбалармен жұмыс істеуге ұқсас, веб-сайттарда аутентификация үшін шаблондар мен профильдер жасалады. Internet Explorer-де аутентификацияны қажет ететін веб-сайтты ашыңыз, оған шаблон жасаңыз. Үлгіні "профиль параметрлері" астында сақтамас бұрын, осы шаблон негізінде жасалған профильді өңдеуге ("қосылатын профильді өңдеу") және жоюға ("қосылатын профильді жою") мүмкіндік беретін параметрлерді өшіріңіз (сурет. 13). Үлгіні "Менің құжаттарым \ eToken SSO Client Templates" ішінде сақтаңыз. Осы шаблон негізінде eToken-де профиль жасаңыз және оны eToken SSO Client арқылы жоюға және өңдеуге тырысыңыз.



Сурет. 13-үлгіні жасау кезінде Профильді өңдеуге және жоюға тыйым салу

Веб-сайт профильдерін жасау үшін шаблондарды қолданудың қажеті жоқ. Профильдерді құру Internet Explorer-де жұмыс істеген кезде тікелей мүмкін болады. Аутентификация деректерін енгізу өрістері бар Интернеттегі кез келген бетті ашыңыз. Логин мен парольді енгізіңіз, содан кейін SSO құралдар тақтасындағы "Сақтау" түймесін басыңыз (сурет. 14). Профильді сақтау кезінде келесі параметрлерді өзгертуге болады: Профиль атауы, пайдаланушының аутентификациясы және енгізуді автоматты түрде растау (сурет. 15). Сайтқа арналған деректерді қамтитын Профильді eToken-ге сақтаңыз. Сонымен қатар, құралдар тақтасы арқылы таңдалған бетке автоматты түрде өту арқылы сақталған веб-сайт профильдеріне жылдам қол жеткізуге болады, сонымен қатар аутентификация формаларын толтыруға және eToken SSO қосуға/өшіруге болады. Веб-сайттар үшін профильдерді автоматты түрде құрудың басты кемшілігі-деректерді енгізу үшін барлық өрістер анықталып, профильге қосылады (мысалы, іздеу сұранысын енгізу өрісі).

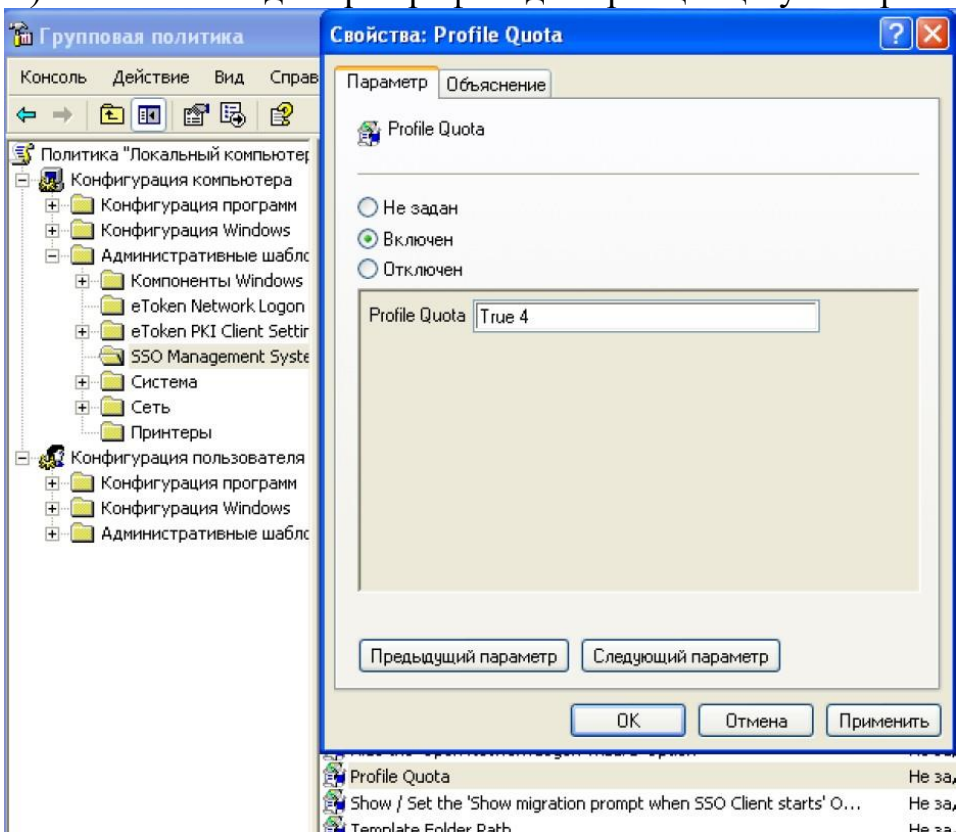
Сурет. 14-Internet Explorer-дегі eToken SSO құралдар тақтасы



Сурет. 15-веб-сайт үшін автоматты профиль жасау

4. EToken SSO әкімшілігі

"EToken SSO Client" утилитасының параметрлерін тиісті әкімшілік үлгіні пайдаланып "топтық саясат" арқылы өзгертуге болады. Gpedit қондырғысын ашыңыз.msc және әкімшілік үлгіні қосыңыз "C:\Program Files\Aladdin\eToken\ eTokenSSO\eTokenSSO.adm». Пайда болған "SSO Management System Settings" бөлімінде кез келген параметрге кіруге рұқсат беруге немесе тыйым салуға, сондай-ақ қарастырылып отырған қызметтік бағдарламаның белгілі бір функцияларын қосуға және өшіруге болады. Мысалы, eToken-де сақтауға болатын профильдер санын шектеңіз. Ол үшін "set a Profiles Quota" параметрінде "True 4" мәнін орнатыңыз (сурет. 16). True-профильдер санына шектеу енгізеді, ал 4-профильдердің максималды санын белгілейді. Енгізілген өзгерістерді тексеру үшін "eToken SSO Client" утилитасын қайта іске қосыңыз ("бастау - бағдарламалар - eToken - eToken SSO - resume eToken SSO Client") және eToken-де төрт профильден артық сақтауға тырысыңыз.



Сурет. 16-eToken - де сақталатын профильдердің максималды санын шектеу

Тапсырма

1. Опцияңызда көрсетілген қолданба терезесі үшін үлгі жасаңыз (кесте. 1).
2. Үлгіні жасау кезінде оған Сіздің опцияңызда көрсетілген параметрлерді орнатыңыз (кесте. 1).
3. Қалыптасқан шаблон негізінде eToken-ге сәйкес профиль жасаңыз және сақтаңыз.

1-кесте-жұмыс нұсқалары

Вар.	***Приложение***	***Настройки шаблона***

1	Ввод пароля на proxy-сервер при запуске Internet Explorer.	Запрет удаления профиля.
2	Ввод пароля на proxy-сервер при запуске Internet Explorer.	Запрет редактирования профиля.
3	Ввод пароля на proxy-сервер при запуске Internet Explorer.	Запрет отображения настроек профиля.
4	Запуск от имени администратора *.	Запрет удаления профиля.
5	Запуск от имени администратора *.	Запрет редактирования профиля.
6	Запуск от имени администратора *.	Запрет отображения настроек профиля.
7	Открытие файла из зашифрованного архива 7-Zip.	Запрет удаления профиля.
8	Открытие файла из зашифрованного архива 7-Zip.	Запрет редактирования профиля.
9	Открытие файла из зашифрованного архива 7-Zip.	Запрет отображения настроек профиля.
10	Добавлениефайлов к зашифрованному архиву 7-Zip.	Отключить автоматическое подтверждение введённых данных.

* - көрсету үшін "User" есептік жазбасына кіріп, "Әкімші"есептік жазбасының атынан кез-келген MMC қондырғысын іске қосыңыз.

Бақылау сұрақтары

1. Пайдаланушылардың жұмыс станцияларындағы әртүрлі қолданбалы бағдарламаларда аутентификация үшін eToken-ді қандай қосымшаның көмегімен пайдалануға болады?
2. EToken SSO қолданатын "қолданба үлгілері" дегеніміз не?
3. EToken - де сақталған профильге не кіреді?
4. Үлгіге қолданба терезесінің өрістері қалай қосылады?
5. "Менің құжаттарым\u003d SSO Templates" және "менің құжаттарым\eToken SSO Client Templates" қалталары не үшін арналған?
6. EToken SSO Client үшін қол жетімді шаблондар тізімін қалай көруге болады?
7. Үлгіні жасау кезінде осы шаблон негізінде жасалған профильді eToken-ден жоюға қалай тыйым салуға болады?
8. EToken профилінде сақталған деректерді қалай өңдеуге болады?
9. Енгізілген деректерді автоматты түрде растау үшін қандай профиль параметрі

жауап береді?
10. Ашық бетке негізделген профильдер жасаумен салыстырғанда шаблонға негізделген веб-сайт профильдерін құрудың артықшылығы неде?

Тапсырма
Зертханалық жұмыс туралы есеп әдістемелік нұсқауларда сипатталған стандарт бойынша орындалады

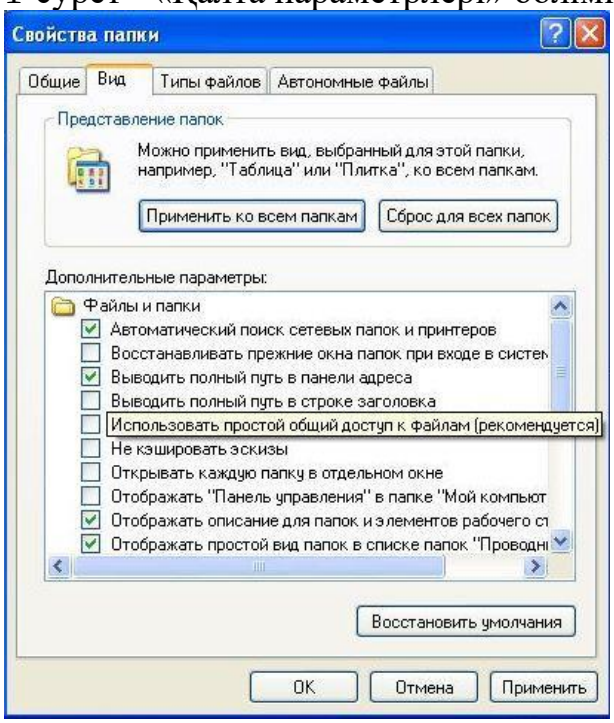
ОЖҚ. Зертханалық жұмыс №10. ФАЙЛ ОБЪЕКТІЛЕРІНЕ ҚОЛ ЖЕТКІЗУДІ ШЕКТЕУДІҢ ДИСКРЕЦИЯЛЫҚ МЕХАНИЗМІ

Бұл жұмыстың мақсаты NTFS файлдық жүйесінің файлдары мен қалталарына қол жеткізуді басқаруға мүмкіндік беретін Windows XP Professional операциялық жүйесінің кіріктірілген құралдары негізінде қол жеткізуді басқарудың дискрециялық механизмін практикалық зерттеу болып табылады.

Жұмыс барысы

«Администратор» арқылы операциялық жүйеге кіріңіз. Қол жеткізуді басқару ережелерін қолдану үшін «Қауіпсіздік(Безопасность)» қойындысын пайдаланыңыз. Ол әдептегі бойынша өшірілгендіктен, оны қосу керек. Ол үшін «Қалта параметрлері (Свойства папки)» бөліміндегі «Файлдардағы қарапайым ортақ пайдалануды пайдалану (Использовать простой общий доступ к файлам)» опциясын өшіріңіз (1-сурет).

1-сурет - «Қалта параметрлері» бөлімі



1. Файлдық объектілерге қол жеткізудің негізгі құқықтары

NTFS жүйесінде барлық рұқсаттар алты стандартты рұқсатқа дейін қысқарады (Толық басқару, өзгерту, оқу және орындау, қалта мазмұнын тізімдеу, оқу, жазу). Бұл рұқсаттар пайдаланушыға (немесе пайдаланушылар тобына) объектілерге – каталогтар мен файлдарға қол жеткізу үшін берілуі мүмкін. «Толық қол жеткізу» құқығы барлық басқа рұқсаттарды ғана қамтып қоймайды, сонымен қатар осы нысанға қол жеткізуді басқаруды басқаруға мүмкіндік береді. Әрбір нысан үшін пайдаланушының қол жеткізу құқықтары тағайындалады.

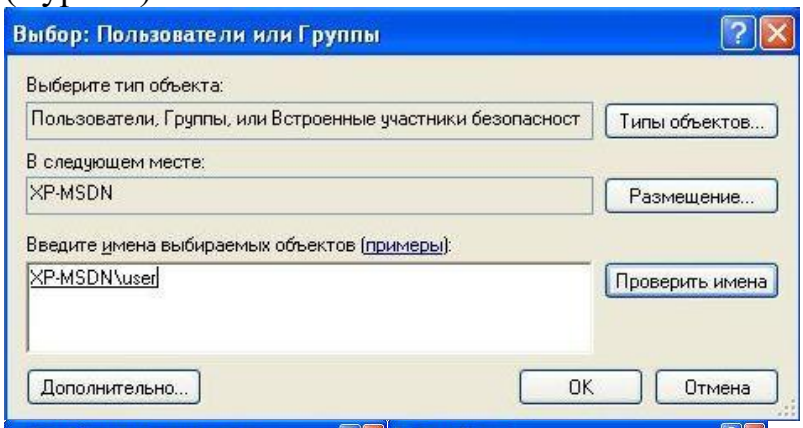
Әрбір нысан үшін пайдаланушының қол жеткізу құқықтары тағайындалады. «Қауіпсіздік» қойындысындағы таңдалған каталогтың немесе файлдың «Сипаттар» бөлімінде қол жеткізу құқықтарын тағайындауға немесе өзгертуге болады. Алдымен рұқсаттар тағайындалатын пайдаланушыны (немесе топты) таңдау керек.

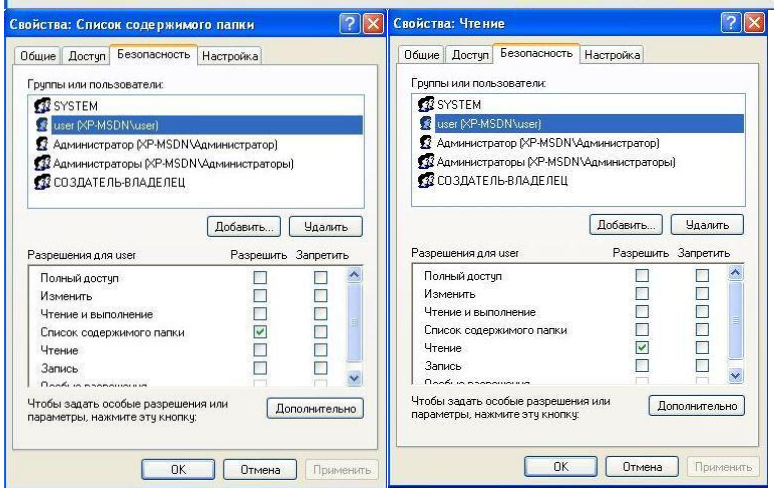
"D:\Folder Contents List" каталогының "Сипаттар (Свойствах) " бөлімінде "Қауіпсіздік (Безопасность)" қойындысын ашыңыз. Объектіге кіру құқығы бар пайдаланушылар тізімін өзгерту үшін «Қосу» түймесін басып, «пайдаланушы» пайдаланушыны

таңдаңыз (2-сурет).

2-сурет - Жаңа пайдаланушыны қосу

Ағымдағы «D:\List Folder Contents» каталогына кіру үшін «Пайдаланушының(User)» «Қалта мазмұнының тізімі (Список содержимого папки)» рұқсатын орнатыңыз (Сурет 3).

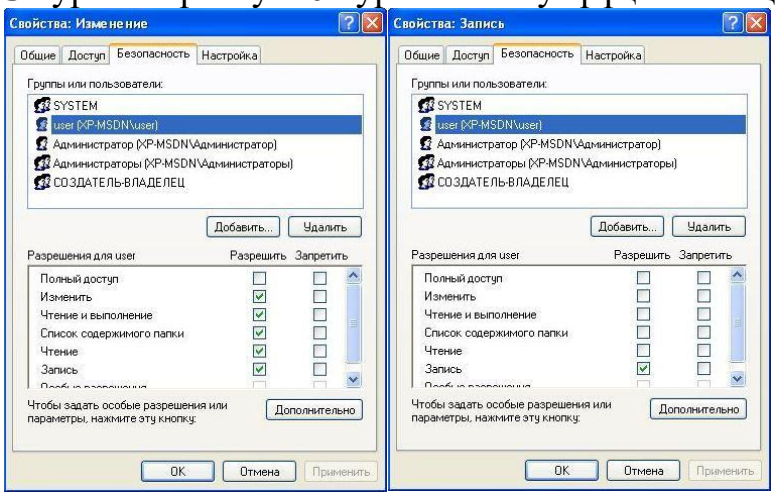


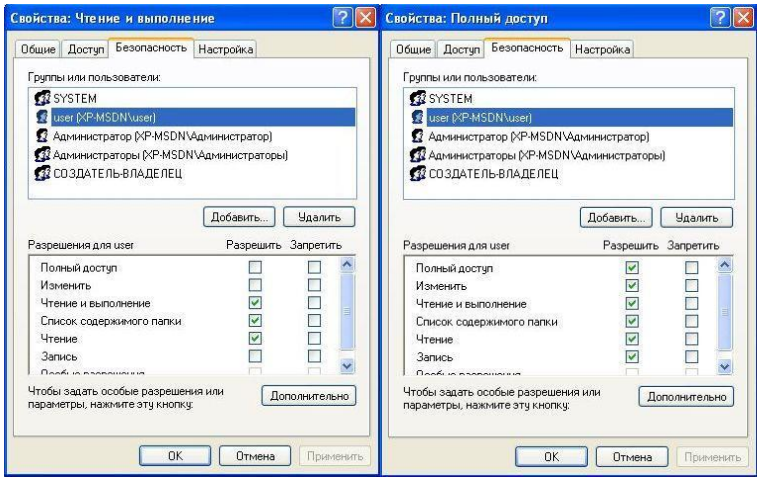


3-сурет - Орнату 4-сурет - «Тізім мазмұнын «оқу» қалталар» рұқсатын орнату

Сол сияқты, «Оқу», «Оқу және орындау», «Жазу», «Өзгерту» және «Толық басқару» каталогтарында «пайдаланушы(user)» пайдаланушысы үшін осы каталогтардың атына сәйкес рұқсаттарды орнатыңыз (4-8-сурет).

5-сурет - Орнату 6-сурет - "Жазу" рұқсатының "Өңдеу" рұқсатын орнату



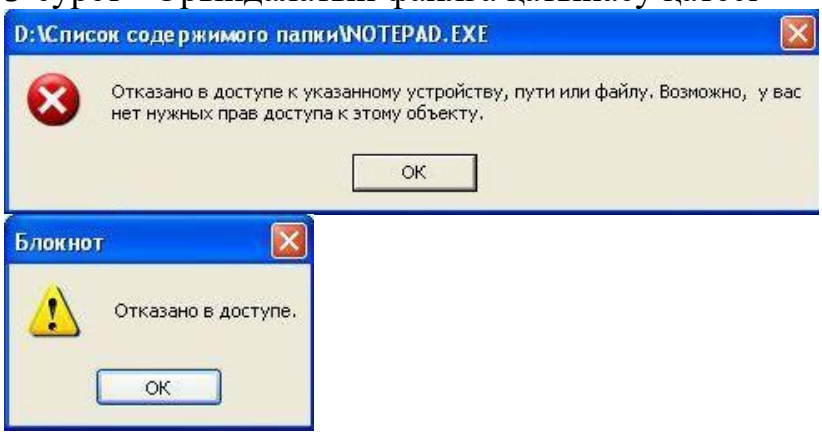


7-сурет - Орнату 8-сурет - «Оқу» рұқсатын және «Толық рұқсат» рұқсатын орнату орындау»

Көрсетілген каталогтарға рұқсаттарды орнату кезінде пайдаланушыға берілген кіру құқықтарын тексеру үшін «пайдаланушы» тіркелгісімен кіріңіз.

Тізім қалтасының мазмұны рұқсаты берілген каталогтағы нысандар тізімін көру мүмкіндігін береді. Сәйкес каталогқа ауысып, орындалатын файлды іске қосып көріңіз. Операциялық жүйе бұл файлға қатынасу кезінде қате береді (Сурет 9). Мәтіндік файлды ашып көріңіз. Операциялық жүйе де кіру қатесін береді (Сурет 10).

9-сурет - Орындалатын файлға қатынасу қатесі



10-сурет - Мәтіндік файлға қатынасу қатесі

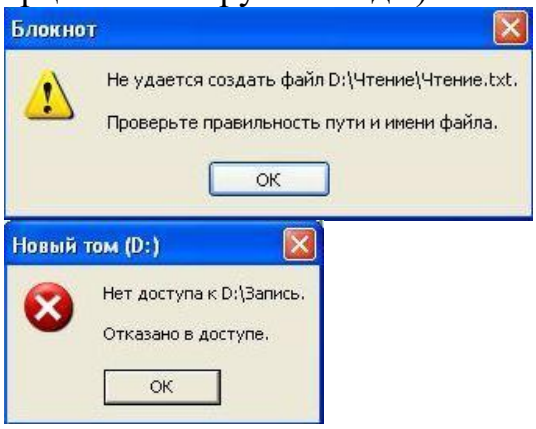
«Оқу» рұқсаты осы каталогтағы орындалатын файлдарды қоспағанда, барлық файлдарды ашу мүмкіндігін береді. Тиісті каталогты енгізіп, мәтіндік файлды ашыңыз. Ашық файлдағы мәтінді өзгертіп, оны сақтауға тырысыңыз. Операциялық жүйе файлды жасау үшін кіру қатесін береді (Сурет 11). Рұқсат етілмеуін тексеру үшін орындалатын файлды іске қосып көріңіз.

11-сурет - Өзгертілген мәтіндік файлды құру және сақтау үшін қол жеткізу қатесі

Оқу және орындау рұқсаты берілген каталогтағы барлық файлдарды ашу мүмкіндігін береді. Сәйкес каталогқа ауысып, орындалатын файлды іске қосыңыз. Мәтіндік файлды ашыңыз, ондағы мәтінді өзгертіңіз және сақтау рұқсатына тыйым салынғанын тексеру үшін сақтап көріңіз.

«Жазу» рұқсаты файлдарды осы каталогқа оның ішінде кірістірілген нысандарға қатынасу құқығынсыз қосу мүмкіндігін береді. каталогтың мазмұнын көру үшін. Тиісті каталогты енгізуге тырысыңыз. Операциялық жүйе каталогқа кіру қатесін

береді (Сурет 12). Файлды қосу мүмкіндігін тексеру үшін «Жазба» деп аталатын файлды жасаңыз (мысалы, «Жұмыс үстелінде») және оны «Жазба» каталогына апарып көріңіз. Операциялық жүйе көшіру қатесін береді, себебі. каталогта осындай атау бар файл бар. Файлдың атын өзгертіңіз және оны қайтадан сүйреп көріңіз - көшіру аяқталады (сонымен қатар, каталогта файлдың болуын «Әкімші» тіркелгісі арқылы тексеруге болады).

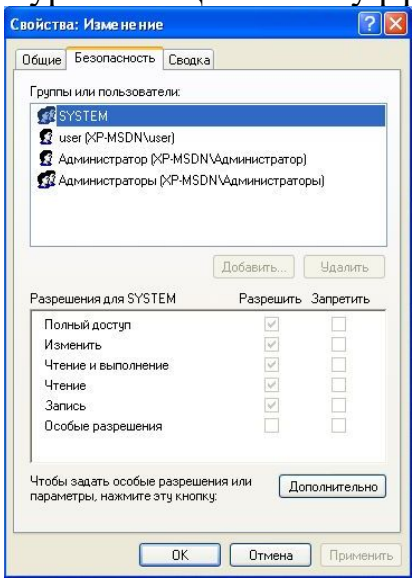


12-сурет - Каталогқа кіру қатесі

Өңдеу рұқсаты берілген каталогта файлдарды ашу және жасау (өзгерту) мүмкіндігін береді. Сәйкес каталогқа ауысып, орындалатын файлды іске қосыңыз. Мәтіндік файлды ашыңыз, ондағы мәтінді өзгертіңіз және сақтаңыз, каталогта жаңа файл жасаңыз. «Өзгерту» каталогының немесе кез келген тіркелген файлдың «Қауіпсіздік» қойындысын ашып, ондағы рұқсаттарды өзгертуге тырысыңыз. Қол жеткізу құқықтарын өзгерте алмайсыз (қосу рұқсаттары опциялары сұр түсті), себебі «Өзгерту» рұқсаты қол жеткізу құқықтарын басқару мүмкіндігін қамтымайды (Сурет 13).

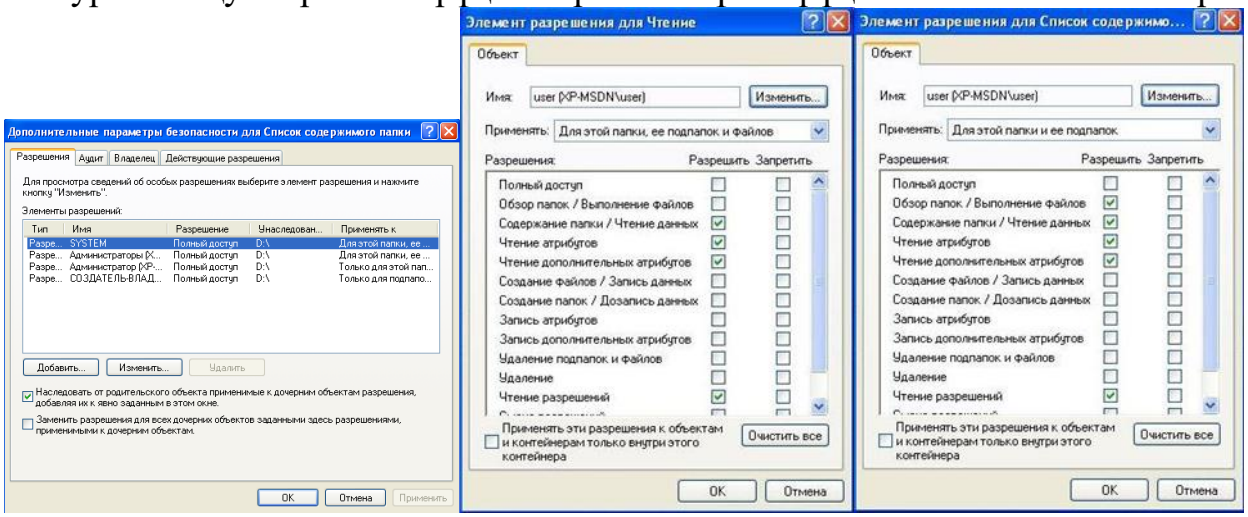
Толық басқару рұқсаты рұқсаттарды өзгертуді қоса, каталог пен оның тіркелген файлдарын толық бақылауға мүмкіндік береді. Тексеру үшін «Толық басқару» каталогының немесе кез келген тіркелген файлдың «Қауіпсіздік» қойындысын ашып, оған кіру құқықтарын өзгертіңіз.

Сурет 13 - Қол жеткізу рұқсаттарын өзгерту мүмкін емес

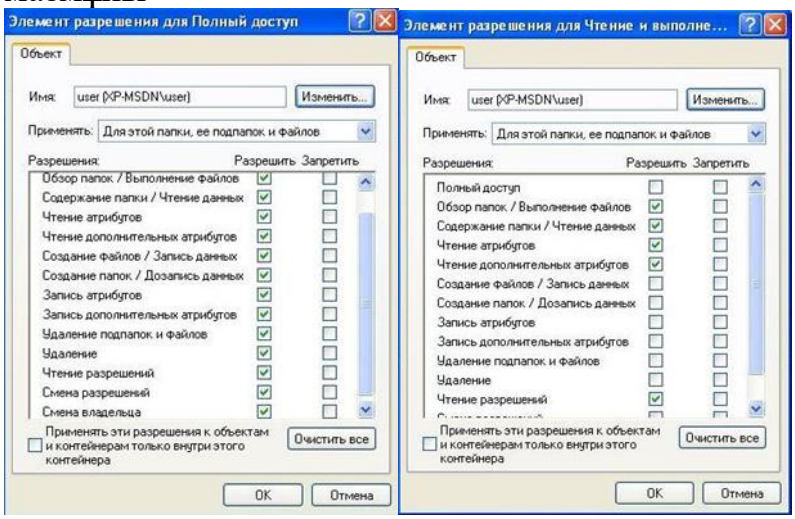


2. Қатынас рұқсаттарының элементтері

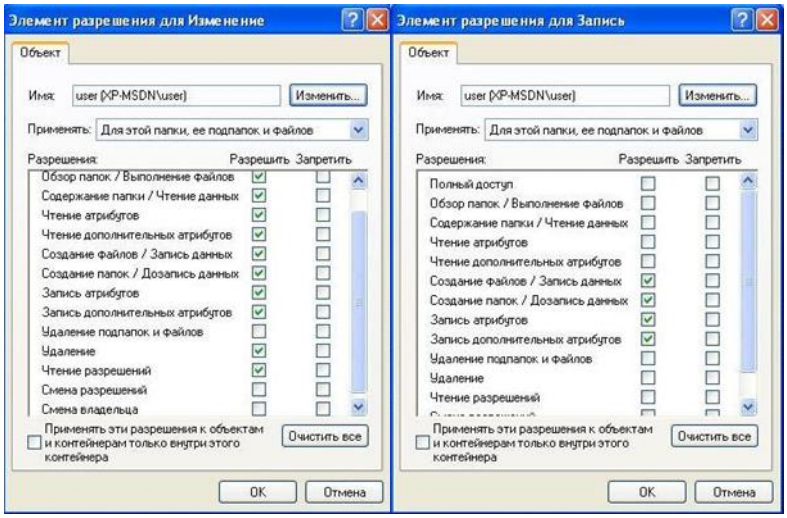
Әрбір стандартты ажыратымдылық бірнеше элементтерден тұрады. Рұқсат элементтері пайдаланушының кіру құқықтарын икемді конфигурациялауға мүмкіндік береді.
«Әкімші» тіркелгісі арқылы кіріңіз.
«Қауіпсіздік» қойындысындағы «Қосымша» түймесін басу және кез келген рұқсат элементін таңдау арқылы қол жеткізуге рұқсат элементтерін көруге болады (Сурет 14). Стандартты рұқсаттарға енгізілген элементтер жиыны күріште көрсетілген. 15-20.
14-сурет - Қосымша қауіпсіздік параметрлері
15-сурет-Элементтер
16-сурет - "оқуға арналған рұқсаттар тізімі "үшін рұқсат етілген элементтер



бума мазмұны"



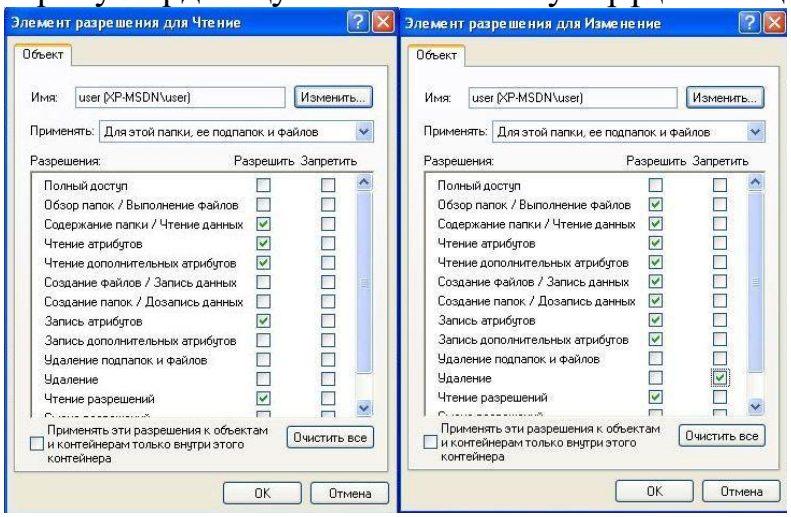
17-сурет - "оқу және орындау"үшін рұқсат етілген элементтер
18-сурет - "толық қол жеткізу"үшін рұқсат етілген элементтер



19-сурет - "өзгерту" үшін рұқсат етілген элементтер

20-сурет - "жазуға" рұқсат етілген элементтері

Рұқсат етілген элементтердің мүмкіндіктерін пайдалану файлды немесе каталогты жоюға қол жеткізуді бөлу кезінде негізделген. Рұқсат етілген элементтері арқылы "пайдаланушыға(user)" тыйым салыңыз өзгерту каталогын жойыңыз, сонымен қатар атрибуттарды оқу каталогына жазуға рұқсат етіңіз (сурет. 21-22).

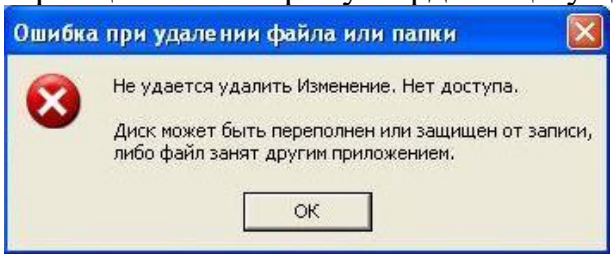


21-сурет-жоюға тыйым салу

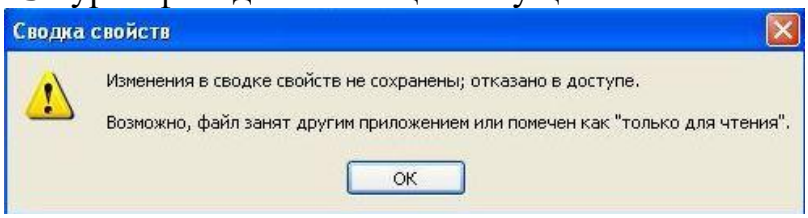
22-сурет-атрибуттарды жазуға рұқсат беру

Орнатылған кіру құқықтарын тексеру үшін "пайдаланушы(user)"есептік жазбасына кіріңіз. Файлды өзгерту каталогынан жоюға тырысыңыз. Амалдық жүйе файлды жоюға қатынасу қатесін береді (сурет. 23).

Оқу каталогындағы файл атрибуттарын өзгертіңіз (мысалы, файл қасиеттеріндегі жасырын атрибут). Өзгерістерді қолданыңыз. Оқу каталогындағы мәтіндік файлдың қосымша атрибуттарын өзгертіңіз (мысалы, файл қасиеттерінің қысқаша мазмұны қойындысындағы құжат авторы). Өзгерістерді қолдануға тырысыңыз. Амалдық жүйе қосымша атрибуттарды сақтау қатесін береді (сурет. 24).



23-сурет-файлды жоюға қатынау қатесі



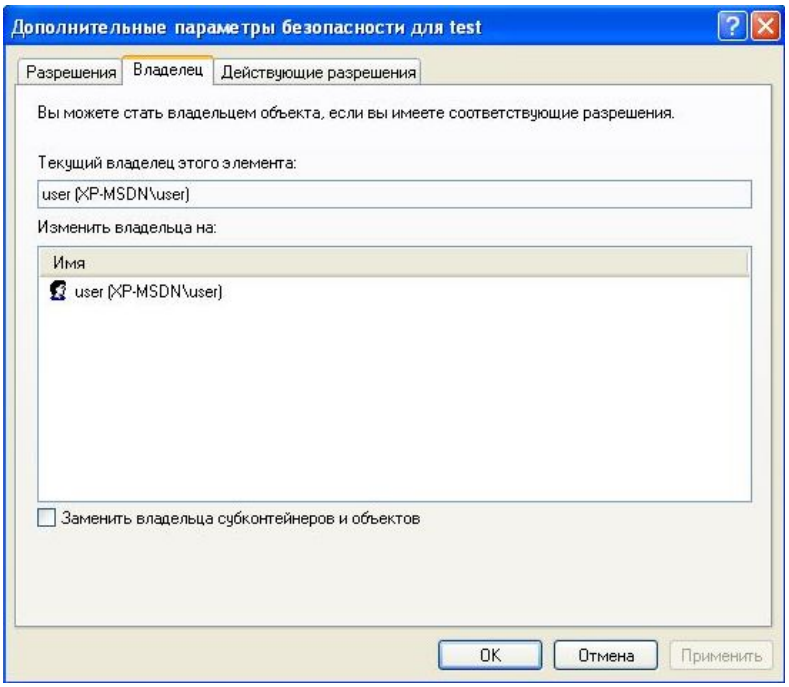
24-Сурет-Қосымша атрибуттарды өзгертуге қол жеткізу қатесі

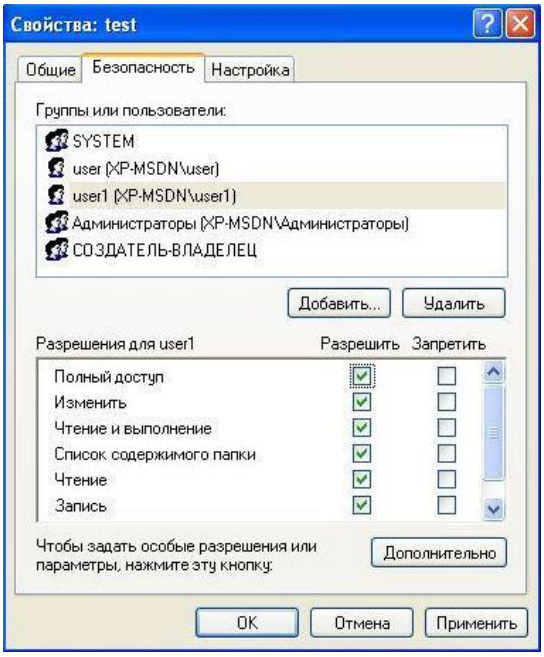
3. Файлдың "иесі"

NTFS файлдық жүйесінде әр объектінің иесі болады. Иесі белгіленген рұқсаттарға қарамастан объектіге кіруге рұқсаттардың мақсатын басқарады.

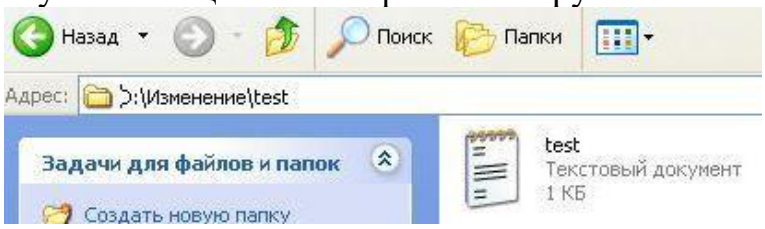
"User" есептік жазбасында "өзгерту" каталогында жаңа каталог (мысалы," test") және мәтіндік файл (мысалы, " test.txt») жасаңыз. Жасалған мәтіндік файлға ақпаратты өзгерту файлынан көшіріңіз. Test файлының иесі қойындысын ашыңыз.txt». Онда объектінің ағымдағы иесі көрсетіледі (сурет. 25). "User1" пайдаланушысына жасалған каталогқа толық қол жеткізіңіз (сурет. 26).

25-Сурет - "Иесі(владелец)" қыстырма беті

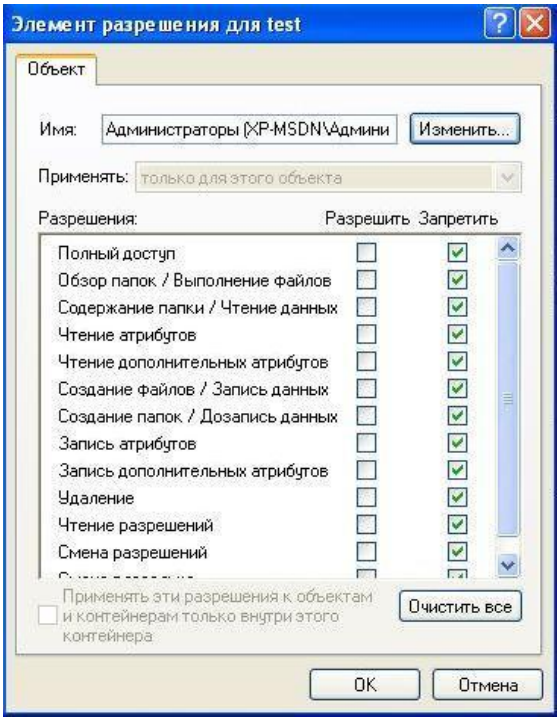




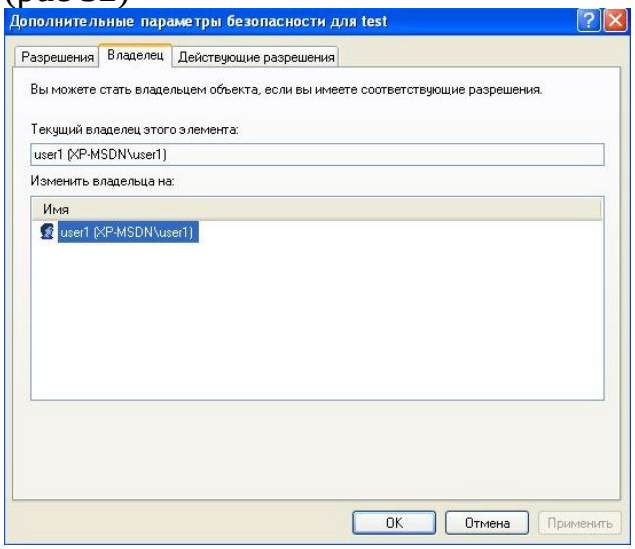
Сурет 26 - Пайдаланушыға құқықтарды беруl> «user1» тіркелгісімен кіріңіз. Explorer бағдарламасындағы Перархиялық каталог көрінісі арқылы D:\Change> каталогына өтіп көріңіз. Өту мүмкін емес, себебі "user1" пайдаланушысы аралық каталогтарға қол жеткізе алмайды. «Explorer» (Сурет 27) мекенжай жолағында оның толық жолын көрсету арқылы сол каталогқа өтуге тырысыңыз. «test.txt» файлын ашыңыз. Осылайша, пайдаланушы «пайдаланушы» рұқсатсыз болуы мүмкін. "user1" пайдаланушыға құпия ақпаратқа рұқсат беру. «user1» пайдаланушысының «<test>> каталогына толық қол жеткізу фактісі оған рұқсаттарды өзгертуге мүмкіндік береді. <<Әкімші» пайдаланушысының «test.txt» файлына кіруіне тыйым салу (Сурет 28)



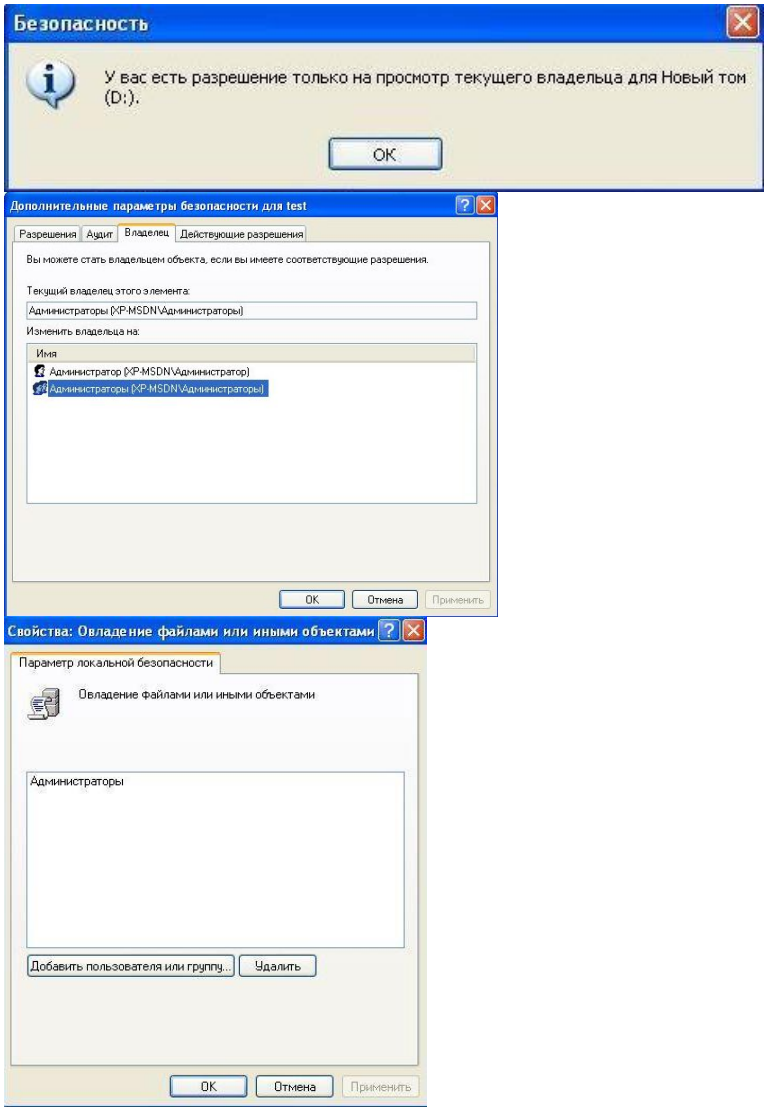
Сурет-27



28-сурет - Файлға кіруге тыйым салу "Толық" қосымша рұқсат файлды өзгерту мүмкіндігін береді. “test.txt” файлының иесін user1 етіп өзгертіңіз” (Сурет 29). Толық қол жеткізе алмайтын басқа файлдың/каталогтың иелігін өзгертіп көріңіз (мысалы, D:\ дискісі). Операциялық жүйе қате атауын береді иесі (Сурет 30). Әкімші тіркелгісімен кіріңіз. «test tat» файлына қол жеткізіп көріңіз. Ast файлға қол жеткізе алса да, ол файлдың регистрлерін өзгерте алады.Файлдың сипаттарын жабыңыз. Файлды жіберген кезде пайдаланушының кіру құқықтарын орнату мүмкіндігі бар (31) Пайдаланушылардың толық рұқсатсыз иесін өзгертуге құқығы жоқ. obsexTamm (рис 32)



29-сурет – Файлдың иесін өзгерту
31-сурет – «Әкімшілер» тобын файл иесі ретінде орнату
30-сурет - Файл иесін өзгерту қатесі



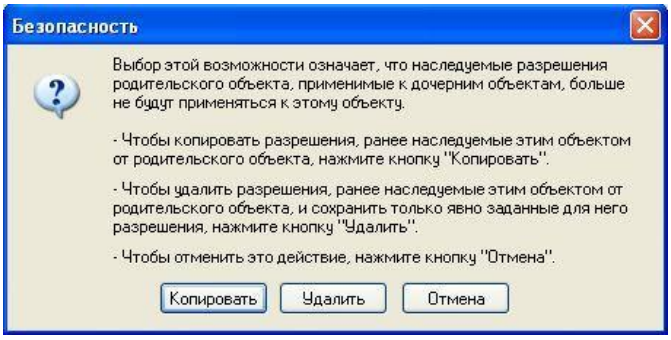
32-сурет - «Файлдарға және басқа объектілерге меншік құқығы» опциясы

4. Қол жеткізу құқықтарының мұрагерлік

NTFS рұқсат мұрасын қолдайды, яғни әдепкі бойынша каталог рұқсаттары оның барлық файлдары мен ішкі каталогтарына таралады. Негізгі каталог рұқсаттарына жасалған кез келген өзгертулер оның ішкі нысандарында көрсетіледі.
Сондай-ақ, мұраға алынған рұқсаттарды бүйірден өзгертуге болады
кірістірілген нысан. ашық
қосымша опциялар
"D:\Read\Read1" және өшіріңіз
«Ата-аналық нысаннан еншілес нысандарға қолданылатын рұқсаттарды мұраға алу, оларды осы терезеде нақты орнатылғандарға қосу»). Мұралауды өшірген кезде, ағымдағы рұқсаттарды көшіріңіз (33-сурет).

33-сурет - Мұрагерлік ажыратылған кезде әрекетті таңдау

Қауіпсіздікті мұраға алу каталогындағы рұқсаттар қойындысы.

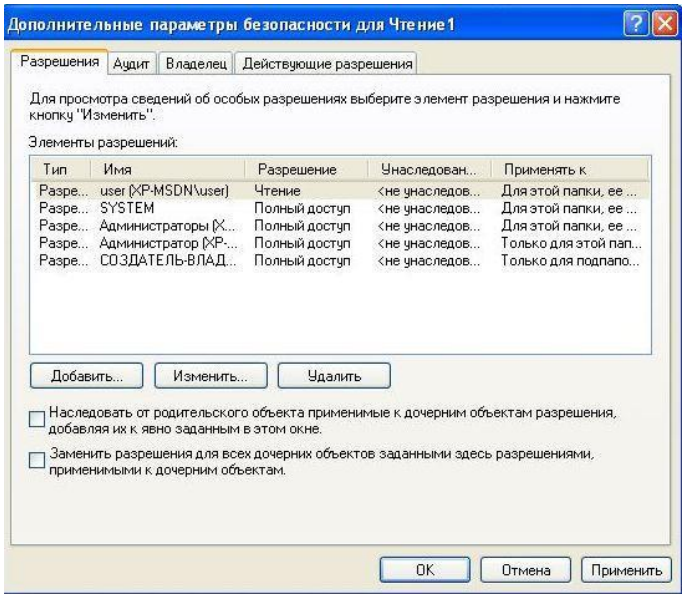


Ата-анадан рұқсаттар каталогы бойынша мұраны өшіргеннен кейін, «Мұрагерлік» бөлімінде әрбір элемент «мұрагерлік емес» күйіне орнатылады (Сурет 34). «Мұрагерлік» бөліміндегі өзгерістердің сипаттамасы.

34-сурет - мұрагерлігі ажыратылған рұқсат элементтері

«Барлық еншілес нысандардағы рұқсаттарды еншілес нысандарға қолданылатын осында орнатылған рұқсаттармен ауыстыру» опциясын пайдаланып кірістірілген нысандардың тиімді рұқсаттарын өзгертуге болады. «Reading1» каталогының рұқсат етілген пайдаланушылар тізімінен «пайдаланушы» тіркелгісін алып тастаңыз. Оның «Оқу» басты каталогында еншілес объектілердің құқықтарының өзгеруін орнатыңыз (Сурет 35). «Reading1» каталогының рұқсат етілген пайдаланушылар тізімінде «пайдаланушы» тіркелгісін қалпына келтіруді тексеріңіз.

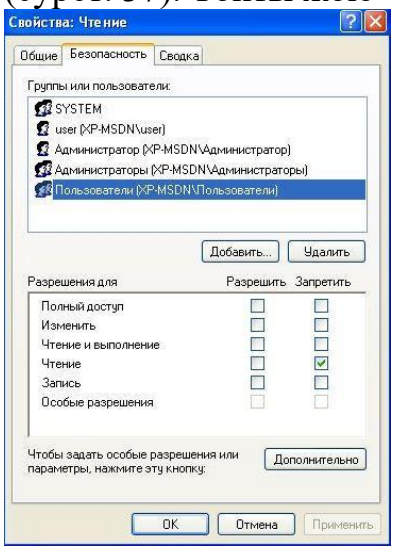
Элементтерге қол жеткізу құқықтарын орнату кезінде сіз рұқсаттарды ғана емес, сонымен қатар тыйым салуларды да орнатуға болады. «Пайдаланушы» мүшесі болып табылатын «Пайдаланушылар» тобына («пайдаланушы» тіркелгісін оқуға рұқсат етіледі) «Оқу» файлын оқуға тыйым салынады (Сурет 36). «Пайдаланушы» тіркелгісімен кіріңіз. Reading файлын ашып көріңіз. Файлды ашу мүмкін еместігі тыйымдардың рұқсаттардан басым болуына байланысты.



35 – сурет - Мәжбүрлі мұрагерлікті қосу

36-сурет- оқуға тыйым салуды орнату

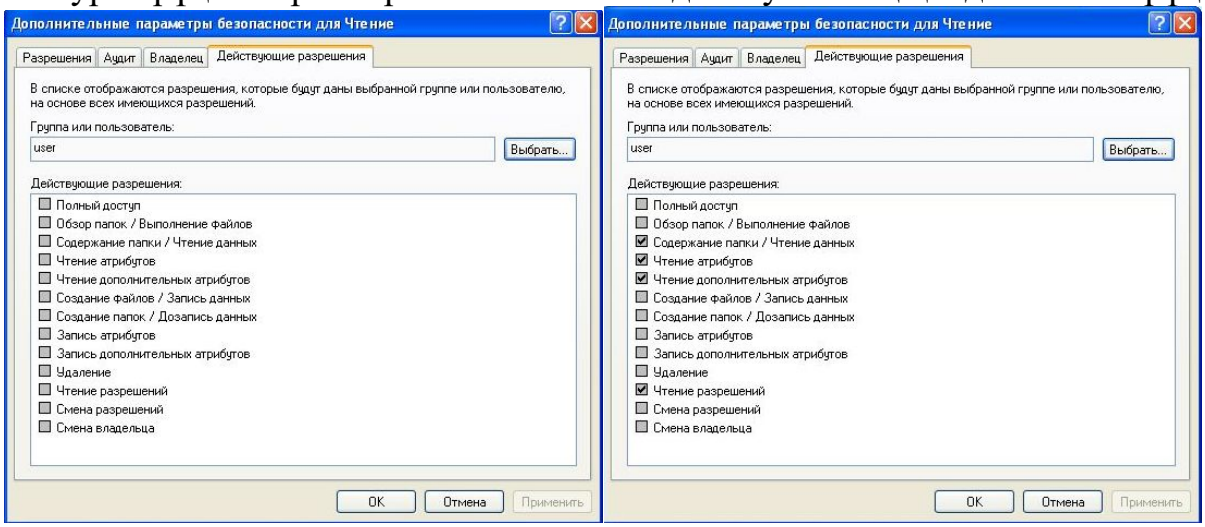
Қолданыстағы рұқсаттарды қосымша қауіпсіздік параметрлері қойындысынан қызығушылық танытқан пайдаланушыны немесе топты таңдау арқылы көруге болады. «Әкімші»(«Администратор») тіркелгісімен кіріңіз. Пайдаланушы (user) үшін "оқу" файлының қолданыстағы рұқсаттарын қарап шығыңыз
(сурет. 37). Топты жою



Рұқсаттар тізімінен "пайдаланушылар". Пайдаланушы «user» рұқсаттарын қайта қарап шығыңыз (сурет. 38). Осылайша, пайдаланушыға және оған кіретін топқа берілген рұқсаттар жинақталады. Пайдаланушылар тобына оқуға тыйым салатын элементті жойғаннан кейін "Пайдаланушы" («user»)Пайдаланушысы тек өз құқықтарын сақтап қалды.

37-сурет-пайдаланушының қолданыстағы рұқсаттары

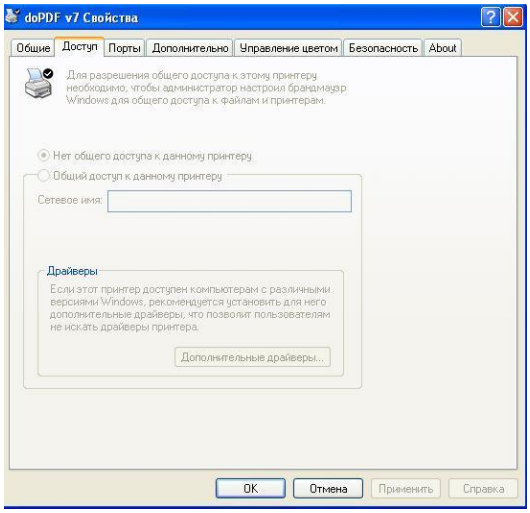
38-сурет-рұқсаттар өзгергеннен кейін пайдаланушының қолданыстағы рұқсаттары



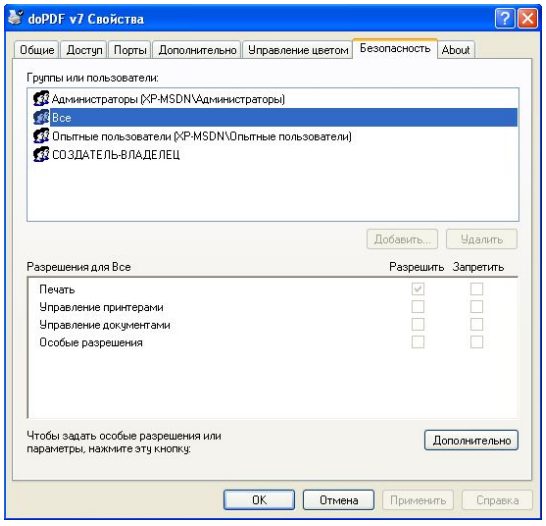
Рұқсаттарды қою кезінде мұраның тереңдігін және объектілердің түрлерін көрсетуге болады. Сіз осы каталогқа орнатылған рұқсаттарды тек кірістірілген нысандарға немесе каталогқа және оның барлық кірістірілген объектілеріне тарата аласыз, сонымен қатар кірістірілген каталогтарды көрсете аласыз немесе файлдар рұқсаттарды таратады.

"Пайдаланушы"(«user») пайдаланушысына "оқу" каталогына тек осы каталогқа салынған ішкі қалталар үшін қалталар жасауға рұқсат етіңіз (сурет. 39), яғни "оқу" және "Оқу2" каталогтарында ішкі қалталарды жасауға тыйым салынады, ал "Оқу1" каталогында ("оқуға" тікелей енгізілген) рұқсат етіледі. "Пайдаланушы" («user»)

есептік жазбасына кіріңіз. Барлық көрсетілген каталогтарда қалталарды жасау мүмкіндігін тексеріңіз.
39-сурет-мұрагерлік объектілерінің тереңдігі мен түрін таңдау
5. Принтерлерге кіруді шектеу
"Пайдаланушы" («user») есептік жазбасында doPDF принтерін пайдаланып мәтіндік файлды басып шығаруға жіберіңіз.
Бастау мәзірінің "принтерлер мен факстар" бөлімінде принтер параметрлерін өзгертуге тырысыңыз (сурет. 40). Параметрлерді өзгерту мүмкін еместігі "барлығы" тобында тек "Басып шығару" құқығының болуымен түсіндіріледі ("принтерлерді басқару" құқығының болмауы) (сурет. 41).



40-сурет - Принтер сипаттары
41-сурет - Принтерге қол жеткізуді саралау
«Әкімші» тіркелгісі арқылы кіріңіз. doPDF принтеріне кіру тізімінен "Барлығы" тобын алып тастаңыз.
«Пайдаланушы» тіркелгісімен кіріңіз.
Мәтіндік файлды басып шығарып көріңіз. doPDF жоқ «Принтерлер мен факстар» бөлімін ашыңыз, себебі «пайдаланушы емес» принтермен жұмыс істеуге рұқсаты бар пайдаланушылар тізіміне енгізілген.



Жаттығу
«Қоғамдық» және «Құпия» каталогтарын жасаңыз. Осы каталогтардың әрқайсысында орындалатын және мәтіндік файлдарды көшіріңіз. Таңдауыңызға сәйкес принтерге, сондай-ақ жасалған каталогтар мен файлдарға қол жеткізуді шектеңіз.

1-нұсқа Тақырыптар
Нысандар Жалпыға ортақ құпия Оқу рұқсат жоқ Құпия Оқу және орындау Оқу Принтер Толық басқару Басып шығару Принтер Толық басқару Басып шығару

Әкімші Толық басқару user1(пайдаланушы) Өзгерту

user	Оқу	Өзгерту, өшіруден басқа	Басып шығару	Құжаттарды басқару

2-нұсқа Тақырыптар
Объектілер
Қоғамдық
Әкімші - Толық кіру страторы
пайдаланушы Өңдеу

3-нұсқа
Объектілер

user1	Оқу және орындау	Өзгерту Басып шығару Құжаттарды басқару

Тақырыптар
Қоғамдық
Құпия - мәтіндік файл

Әкімші - Толық кіру страторы
пайдаланушы1 Өңдеу
Мазмұн тізімі
Кіру жоқ
«Құпия» Қол жеткізу жоқ
Кіру жоқ

user	Оқу	Өзгерту, өшіруден басқа	Өзгерту

4-нұсқа
Объектілер
Тақырыптар
Қоғамдық
Құпия Оқу және орындау
Өзгерту
Мазмұнның құпия тізімі
«Құпия» ішіндегі мәтіндік файл рұқсат жоқ
Жоюға тыйым салу
«Құпия» бөлімінде орындалатын
Орындау, жоюға тыйым салу
«Құпия» өзгертуінде орындалатын
Орындау Қол жеткізу жоқ
Мәтіндік файл «Қоғамдық»
Кіру жоқ
Әкімші - страторды өзгерту
пайдаланушы оқыды
5-нұсқа
Объектілер

user1	Меншіктің өзгеруін қоспағанда, толық рұқсат	Жазбалар	Кіру жоқ

Тақырыптар

Қоғамдық

Әкімші - Толық кіру страторы
пайдаланушы оқыды
6-нұсқа
Объектілер
Жоюды оқыңыз
Құпия оқу
Және

user1	Өзгерту, өшіруден басқа	Жазбалар	Кіру жоқ

Тақырыптар
Жалпыға қолжетімді
Әкімші-толық қол стратор
user оқу және жою
User1 өзгерту
7 нұсқа
Объектілер
Мазмұн тізіміне кіру жоқ
Конфиденциялық толық қол жетімділік
Субъектілер
Жалпыға қолжетімді

Мазмұн страторының әкімші тізімі

User	Жоюдан басқа өңдеу	Оқу	Өзгерту

user1
Қатынау жоқ
Өңдеу
Құпия Түрде Өзгерту
Қатынау жоқ
"Құпия" ішіндегі мәтіндік файлға қол жетімділік жоқ

8 нұсқа
Объектілер
Субъектілер
Әкімші
Жалпыға қолжетімді
Оқу және орындау

user	Өзгерту	Оқу	Өзгерту, өзгерту тыйымын толықтырады. атрибуттар
user1	Жазу	Өзгерту, басқа жою	Қатынау жоқ

9 нұсқа

Объектілер
Субъектілер
Әкімшілік
user user1
Жалпыға қолжетімді
Конфиденциялық толық қол жетімділік
Оқу
Толық қол жеткізу
Конфиденциялық толық қол жетімділік
Оқу Жою Өзгерту
Орындалатын файл "құпия" орындалуы
Орындау, жоюға тыйым салу
Қатынау жоқ
Орындалатын файл "құпия" өңдеу
Орындау рұқсаты жоқ
Мазмұн тізімі
Оқу жою жазу
және

10 Нұсқа Нысандар

Субъектілер
Жалпыға қолжетімді
Admini-strator оқу
user мазмұн тізімі
user1 қатынау жоқ

Бақылау сұрақтары:
1. Қол жеткізуді басқарудың дискрециялық моделін сипаттаңыз.
2. NTFS файлдық жүйесінде бар файл нысандарына қол жетімділіктің стандартты құқықтарын тізімдеңіз.
3. "Жазу" рұқсатының жұмыс принципін түсіндіріңіз.
4. Рұқсат элементтерін тізімдеңіз.
5. Нысанның иесі кім бола алады?
6. Рұқсат мұрагерлік ұғымын кеңейтіңіз.
7. Рұқсаттарды мұрагерлікті қалай өшіруге болады?
8. Бекітілген рұқсаттардың салынған объектілерін мәжбүрлеп мұрагерлеуді қалай жүзеге асыруға болады?
9. Файл нысандарына кіруге жарамды рұқсаттарды анықтау кезінде рұқсаттарды қолдану басымдықтарын тізімдеңіз.
10. NTFS файлдық жүйесінде бар принтерлерге қол жетімділіктің стандартты құқықтарын тізімдеңіз.

ОЖҚ. Зертханалық жұмыс №11. ФАЙЛДЫҚ ОБЪЕКТІЛЕРГЕ ҚОЛ ЖЕТКІЗУДІ ШЕКТЕУДІҢ МАНДАТТЫҚ МЕХАНИЗМІ

Бұл жұмыстың мақсаты Secret Net 5.1 бағдарламалық өнімі (автономды нұсқа) негізінде қол жеткізуді бөлудің мандаттық механизмін практикалық зерттеу болып табылады.

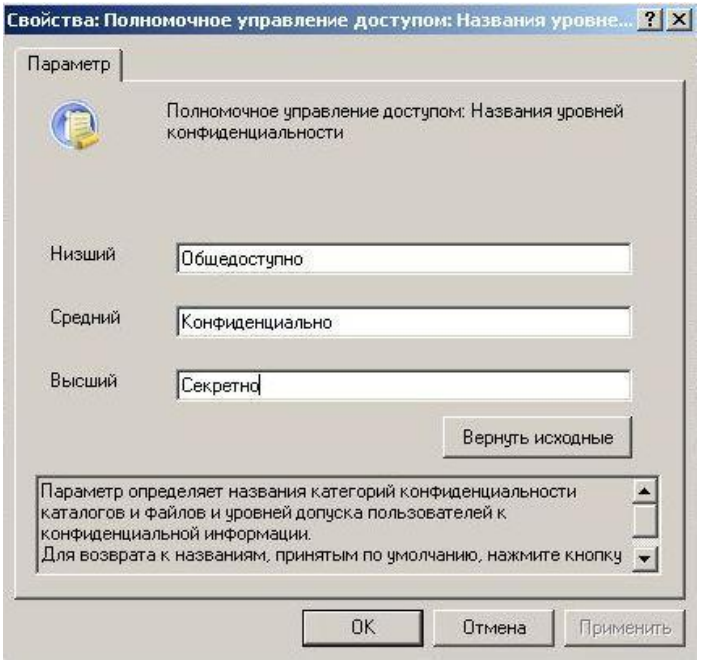
Жұмыс барысы

1. Құпиялылық санаттарын теңшеу

Пайдаланушының осы құжатта қамтылған ақпаратқа қолжетімділігі құпия файл пайдаланушыға тиісті рұқсат деңгейі тағайындалған жағдайда жүзеге асырылады. Жүйеде қолданылатын төзімділік деңгейлерінің жиынтығы ресурстардың құпиялылық санаттарының жиынтығына сәйкес келеді.

Әкімші есептік жазбасында "жергілікті қауіпсіздік параметрлерін" іске қосыңыз: "іске қосу – барлық бағдарламалар – Secret Net 5 – жергілікті қауіпсіздік саясаты", "Secret Net параметрлері 5 ішкі жүйені орнату – ішкі жүйені орнату" тобына өтіңіз.

"Қол жеткізуді басқару: құпиялылық деңгейінің атауы" параметрі суретте көрсетілгендей теңшеңіз.



1-сурет - "құпиялылық деңгейінің атауы"параметрі

2. Қатынау субъектілерін баптау

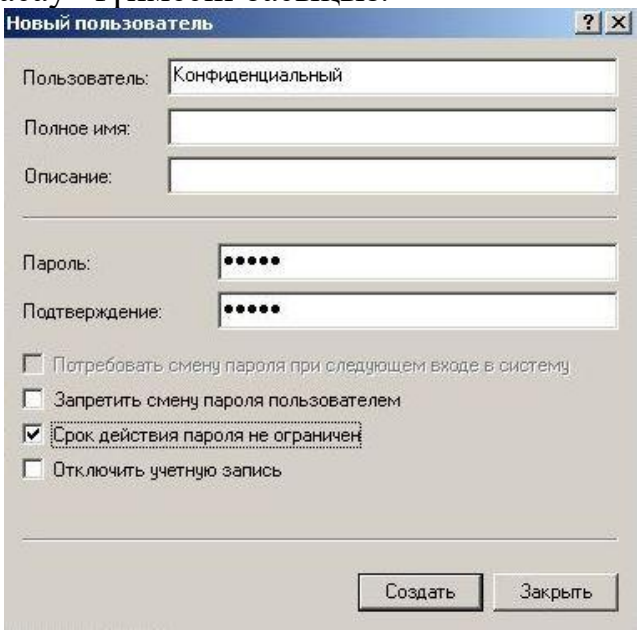
Әкімші тіркелгісінде "компьютерді басқару" іске қосыңыз: "Бастау – Барлық бағдарламалар – Secret Net 5 – компьютерді басқару", "жергілікті пайдаланушылар және пайдаланушы топтар" тобына өтіңіз.

Әрі қарай, әкімші құқықтарын теңшеңіз. Ол үшін Әкімші тіркелгісінің қасиеттерінде Secret net 5 қойындысына өтіңіз. "Кіру" тобында келесі мәндерді орнатыңыз (сурет. 2).

2-сурет - "әкімші"пайдаланушысының кіру құқығын орнату

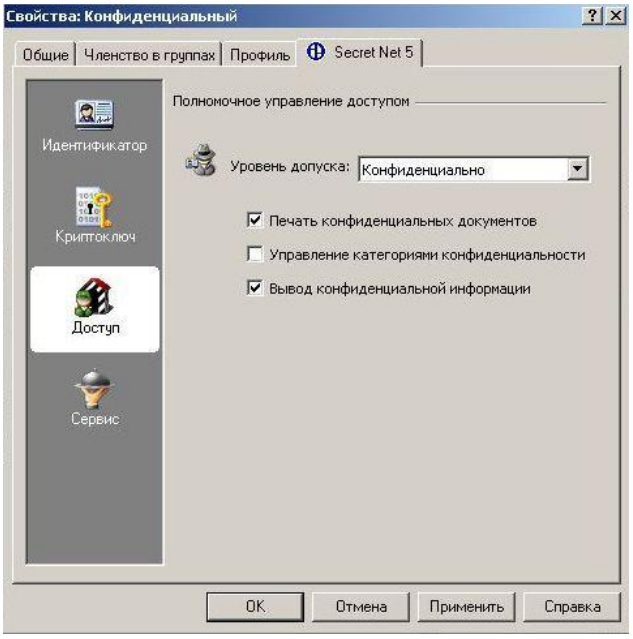
- Құпиялылық санаттарын басқару-пайдаланушы каталогтар мен файлдардың құпиялылық санаттарын рұқсат етілген деңгейде өзгерте алады; каталогтың құпиялылық санаттарының мұрагерлік режимін басқарады.
- Құпия құжаттарды басып шығару-пайдаланушыға құпия құжаттарды принтерге шығаруға рұқсат беру үшін қолданылады. Артықшылық құпия құжаттардың басып шығарылуын бақылау режимі қосылған кезде қолданылады.
- Құпия ақпаратты шығару-пайдаланушыға құпия ақпаратты сыртқы тасымалдағыштарға шығаруға рұқсат етіледі.

Содан кейін "жергілікті пайдаланушылар және пайдаланушы топтар"сериясына оралыңыз. Контекстік мәзірден немесе әрекет мәзірінен жаңа пайдаланушыны таңдау арқылы пайдаланушыны жасаңыз. Есептік жазбаны суретте көрсетілгендей орнатыңыз. 3 және "Жасау" түймесін басыңыз.

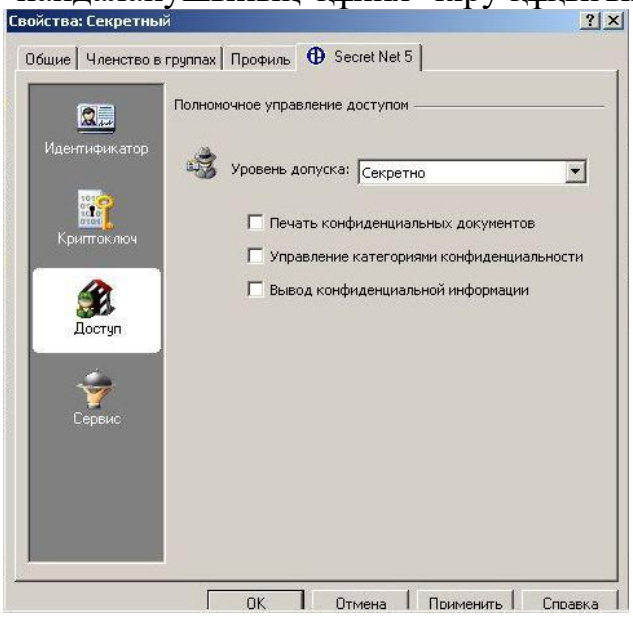


3-сурет-пайдаланушыны құру

Аналогия бойынша "құпия" пайдаланушысын жасаңыз.
Кіру рұқсаттарын орнату үшін "пайдаланушылар" тобына өтіп, пайдаланушыны "құпия"деп таңдаңыз. Мәтінмәндік мәзірден сипаттар таңдаңыз. Кіру тобында параметрлерді суретте көрсетілгендей реттеңіз. 4, ақпаратты сыртқы медиаға шығару және құпия құжаттарды басып шығару құқығын беру.
"Құпия" пайдаланушысы үшін сыртқы тасымалдаушыларға шығаруға және құпия құжаттарды басып шығаруға тыйым салатын "Құпия" рұқсат деңгейін таңдаңыз (сурет. 5).
Параметрлерді қолдану үшін сеансты аяқтап, "Әкімші"есептік жазбасына қайта кіріңіз.

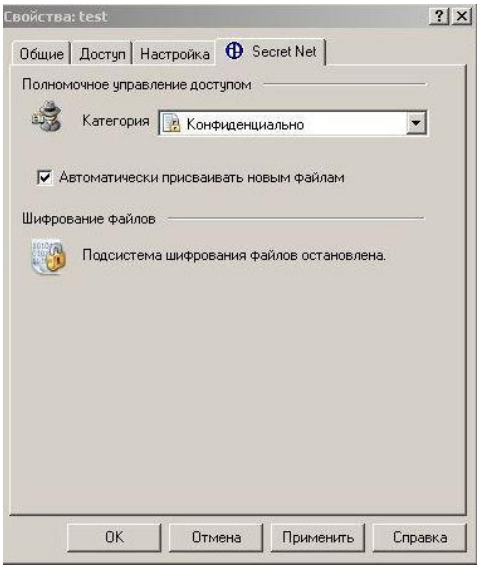


4-сурет - пайдаланушының"құпия" кіру құқығын орнату



5-сурет - "Құпия"пайдаланушының кіру құқығын орнату

3. Кіру нысандарын (деректерді)теңшеу
Қолжетімділікті өкілетті басқару тетігінде құпиялылықтың мынадай санаттары пайдаланылады:
- құпия емес (біздің жағдайда "жалпыға қол жетімді");
- құпия;
- қатаң құпия (біздің жағдайда "құпия").
Құпиялылық санаты ресурс атрибуттарына жатады (каталог немесе файл). Қажетті ресурстардың құпиялылық санаттарын арттыру пайдаланушылар өздерінің қабылдау деңгейлерінде жүзеге асырылады. Уәкілетті қол жеткізуді басқару механизмінде каталогтың құпиялылық санатындағы файлдарды мұрагерлік принципі қолданылады. Жаңа файлдарға каталогтың құпиялылық санатын тағайындау автоматты түрде немесе сұрау бойынша орындалуы мүмкін. Автоматты түрде санат беру режимін қосу және өшіру каталог қасиеттерін теңшеу тілқатысу терезесінде жүзеге асырылады ("Жаңа файлдарға автоматты түрде тағайындау" параметрі, сурет. 6).
Ресурстарға құпиялылық санаттарын беруді "құпиялылық санаттарын басқару" артықшылығы бар уәкілетті пайдаланушылар орындайды. Құпиялылық санатын тек NTFS файлдық жүйесі бар дискілерде орналасқан ресурстарға тағайындауға болады.

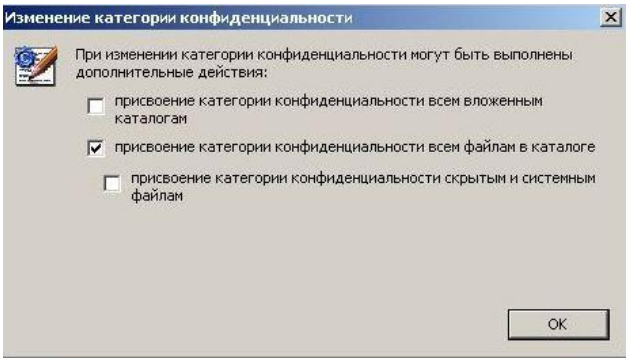


6-сурет-ресурстың құпиялылық санатын таңдау

Каталогтың немесе файлдың құпиялылық санатын қол жеткізуді бөлу режимінде өзгерту үшін "құпиялылық санаттарын басқару"артықшылығы болуы керек. Егер пайдаланушының мұндай артықшылығы болмаса, онда ол тек файлдың құпиялылық санатын арттыра алады, бірақ оның төзімділік деңгейінен немесе сеанстың құпиялылық деңгейінен жоғары емес.
Explorer - де каталогтың контекстік мәзірін шақырыңыз "D:\temp "және"Сипаттар" таңдаңыз. "Сипаттар" терезесінде "құпия жоқ" қойындысын ашыңыз (сурет. 6).
Каталог үшін келесі параметр мәндерін көрсетіңіз:
- ашылмалы тізімнен " санат ""Құпия" санатын таңдаңыз;
- "Жаңа файлдарға автоматты түрде тағайындау"опциясын қосу арқылы каталог файлдарына құпиялылық санатын автоматты түрде тағайындау режимін орнатыңыз.

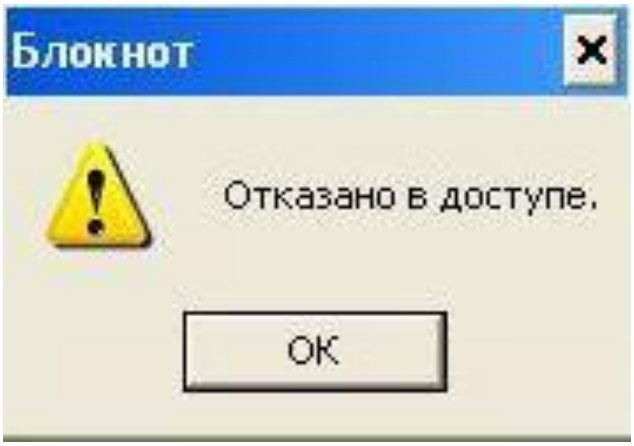
"ОК"түймесін басыңыз.
Егер каталогта файлдар мен ішкі каталогтар болса, экранда кірістірілген файлдар мен каталогтардың құпиялылық санаттарын Өзгертуді ұсынатын диалогтық терезе пайда болады (сурет. 7).

Файлдың құпиялылық санатын өзгерту ұқсас.
Егер пайдаланушының кіру деңгейі файлдың құпиялылық санатынан төмен болмаса, пайдаланушыға файлға кіруге рұқсат етіледі. Мысалы, "Құпия" рұқсаты бар пайдаланушыға "құпия" және "жалпыға қол жетімді" санаттары бар файлдарды оқуға рұқсат етіледі, бірақ "құпия"санаты бар файлдарды ашуға тыйым салынады. "Құпия" кіру деңгейі кез-келген құпиялылық санаты бар файлдарды ашуға мүмкіндік береді.

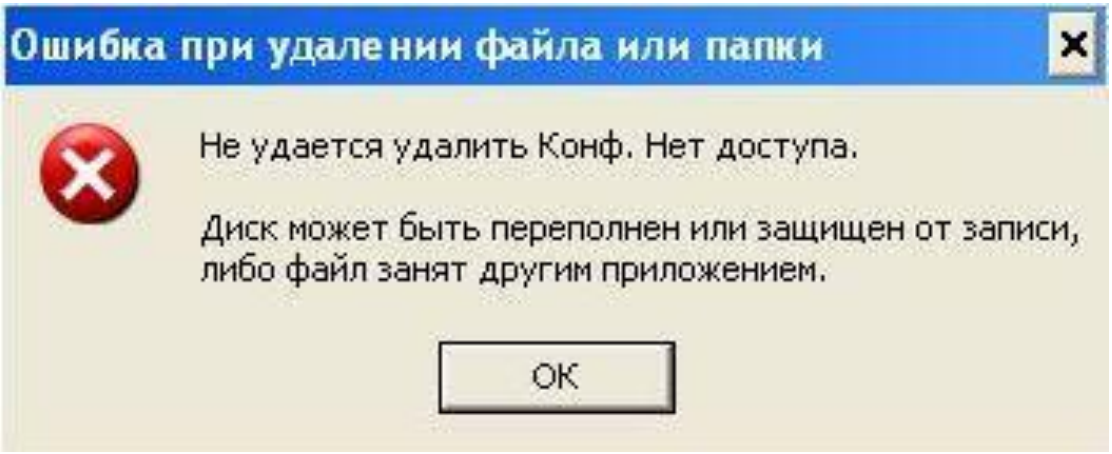


7-сурет-кірістірілген каталогтар мен файлдардың құпиялылық санатын өзгерту

Егер пайдаланушының кіру санаты құжаттар каталогының құпиялылық белгісінен жоғары болса, онда пайдаланушы құжаттарды аша алады, бірақ сол қалтада өзгерте және сақтай алмайды, сонымен қатар құпиялылық санаты пайдаланушының кіру санатынан аз қалталарда құжаттарды құруға және жоюға тыйым салынады.
"Пайдаланушы" есептік жазбасына кіріңіз (кіру деңгейі "жалпыға қол жетімді"). Файлды ашуға тырысыңыз "D:\temp\Конф.txt». Амалдық жүйе осы файлға кіру қатесін береді (сурет. 8). Бұл файлды жоюға тырысыңыз. Амалдық жүйе бұл файлды жою қатесін береді (сурет. 9). Файлды қоғамдық каталогқа көшіруге тырысыңыз (мысалы, "жұмыс үстелі"). Амалдық жүйе файлды көшіру қатесін береді (сурет. 10). "Test" каталогында жаңа файл жасауға тырысыңыз. Амалдық жүйе файл жасау қатесін береді (сурет. 11).
Осылайша, "жалпыға қол жетімді" кіру деңгейі бар есептік жазбада "Құпия" деңгейдегі файлдық нысандармен кез-келген әрекетке тыйым салынады (пайдаланушы құпиялылық санаты рұқсат деңгейінен жоғары құжаттармен жұмыс істей алмайды).



8-сурет-құпия файлға кіру қатесі



9-сурет-құпия файлды жою қатесі

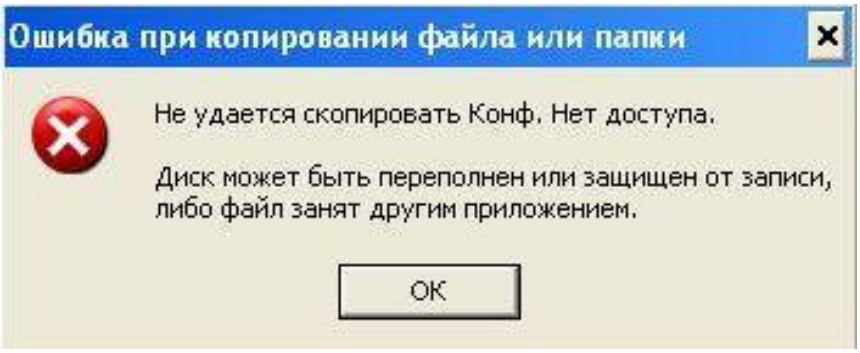
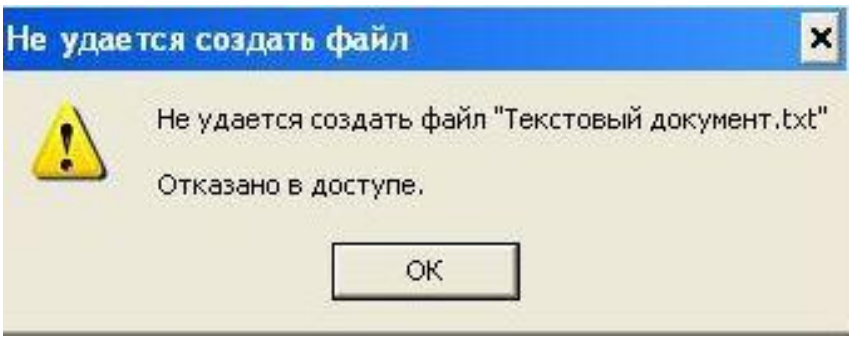
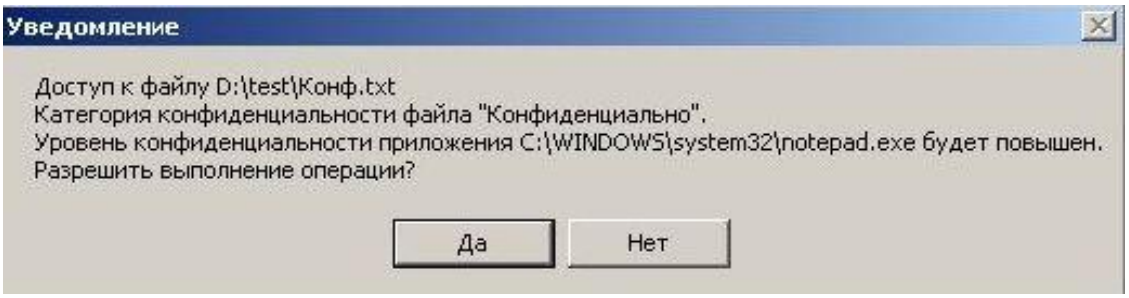


Рисунок 10 – Ошибка копирования конфиденциального файла



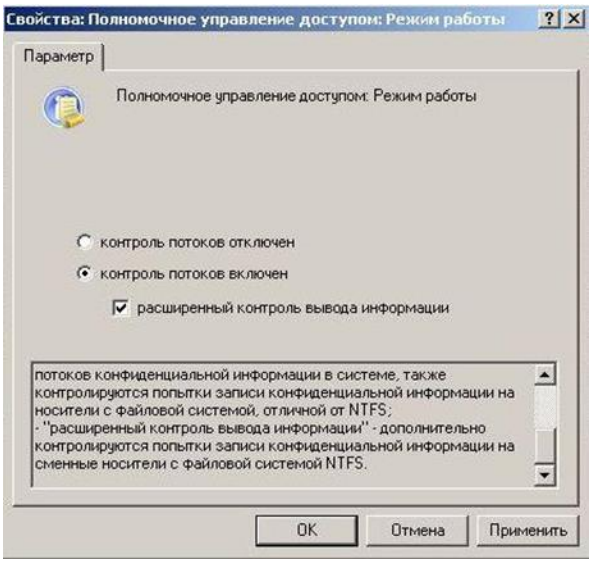
11-сурет-құпия каталогта файл жасау қатесі

"Құпия" есептік жазбасына кіріңіз. Файлды ашуға тырысыңыз "D:\temp\Конф.txt " - қосымшаның құпиялылық деңгейін жоғарылату ұсынысы бар терезе шығарылады (сурет. 12). Файлмен жұмыс істеу деңгей жоғарылағаннан кейін ғана рұқсат етіледі. Файлды қоғамдық каталогқа көшіріңіз (мысалы, "жұмыс үстелі"). Көшірілген файлдың құпиялылық деңгейін қараңыз. Көшіруден кейін "жалпыға қол жетімді"деңгей берілді. Файлдан деректерді көшіруге тырысыңыз "D:\temp\Конф.TXT ""жалпыға қол жетімді" белгісі бар кез келген файлға. Жалпыға қол жетімді файлдың құпиялылық деңгейі өзгерген жоқ.



12-сурет-қосымшаның құпиялылық деңгейін арттыру

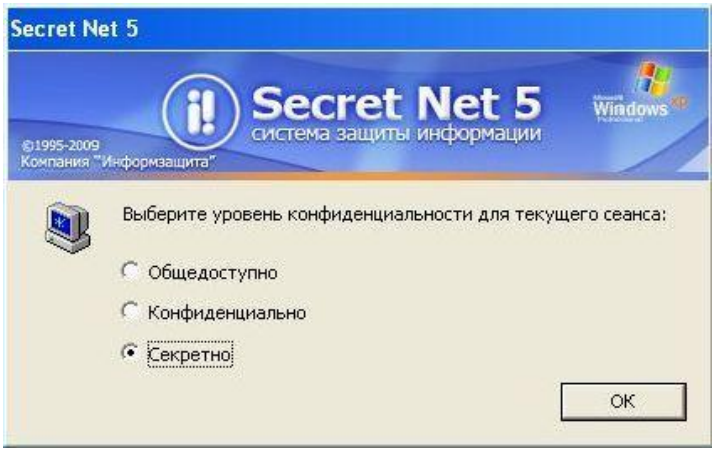
Осылайша, құпия файлдарды жалпыға қол жетімді каталогқа немесе құпия деректердің өздерін жалпыға қол жетімді Файлға көшіру мүмкіндігі ақпараттың ағып кетуіне әкелуі мүмкін.
Осындай тәсілмен ақпараттың құпиялылығы үшін жауапкершілік ақпаратқа қол жеткізуге рұқсат етілген пайдаланушыларға жүктеледі.
4. Деректер ағынын бақылау
4.1. Деректер ағынын бақылауды қосу
Деректер ағынын бақылау арқылы пайдаланушыларға ақпараттың құпиялылық деңгейін төмендетуге тыйым салуға болады.
Әкімші тіркелгісімен кіріңіз. "Жергілікті қауіпсіздік параметрлері" іске қосыңыз: "іске қосу – барлық бағдарламалар – Secret Net 5 – жергілікті қауіпсіздік саясаты", "Secret Net параметрлері – ішкі жүйе параметрлері"тобына өтіңіз. "Қол жеткізуді басқару: жұмыс режимі" опциясын таңдап, ағындарды басқаруды қосыңыз.



13-сурет-деректер ағынын бақылауды қосу

4.2. Сеанстың жоғары деңгейінде құпия файлдармен жұмыс істеу

Параметрлерді қолдану үшін амалдық жүйені қайта іске қосыңыз және "құпия"есептік жазбасына кіріңіз. Кірген кезде жұмыс файл құпиялылығының қай деңгейімен өтетінін анықтайтын сеанс деңгейін таңдау туралы ұсыныс пайда болады (сурет. 14). "Құпия" сеанс деңгейін таңдаңыз.



14-сурет - Сеанстың құпиялылық деңгейін таңдау

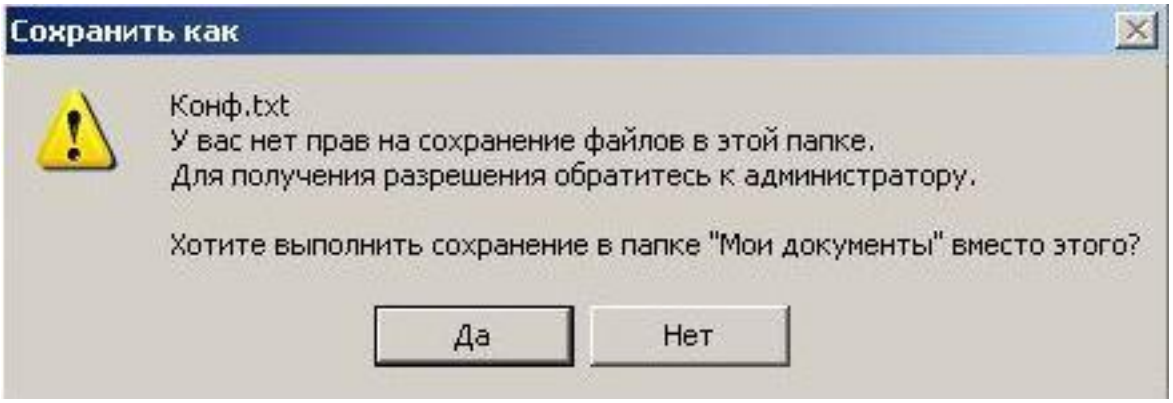
"D:\temp\Conf.txt" файлын ашыңыз. Бұл файлды жойып көріңіз, өзгертіңіз және сақтаңыз, жалпы каталогқа көшіріңіз (мысалы, «Жұмыс үстелі»). «Тест» каталогында жаңа файл жасап көріңіз. Осылайша, егер ағынды басқару қосылса, сеанс деңгейі файлдың құпиялылық деңгейінен жоғары болса, оқудан басқа барлық әрекеттерге тыйым салынады.

"D:\temp\Conf.txt" файлын өзгертіп, оны басқа атпен немесе басқа каталогта сақтап көріңіз. Сақтау мүмкін емес болады (Сурет 15), өйткені сеанс деңгейі каталогтың құпиялылық деңгейінен жоғары.

4.3. Бірдей сеанс деңгейінде құпия файлдармен жұмыс істеу

«Құпия» тіркелгімен кіріп, «Құпия» сеанс деңгейін таңдаңыз.

"D:\temp\Conf.txt" файлын ашыңыз. Осы файлды өзгертіңіз және сақтаңыз, «test» каталогында жаңа файл жасаңыз.



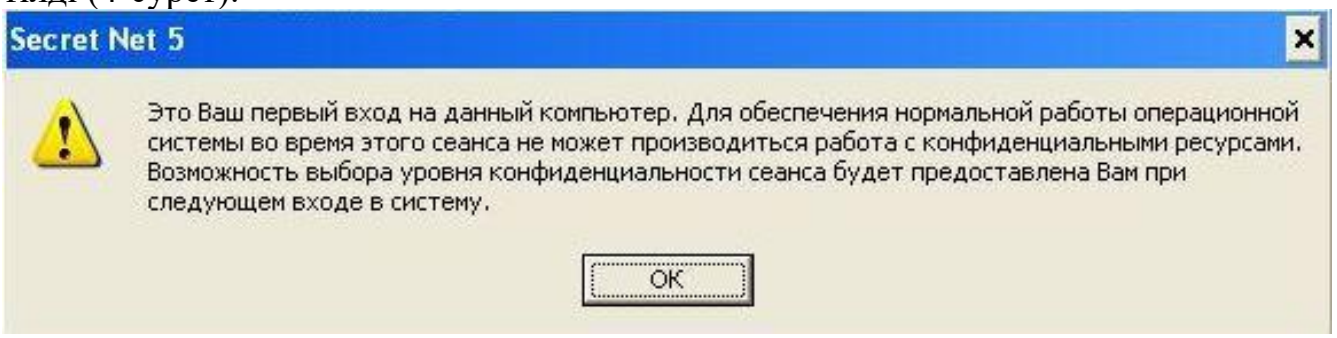
15-сурет - Сеанс деңгейінен төмен құпиялылық деңгейі бар каталогқа ағындарды басқару кезінде ақпаратты сақтау қатесі

Оны жалпы каталогқа көшіріп көріңіз (мысалы, «Жұмыс үстелі»).
Мәтінді «Conf.txt» файлынан «General.txt» файлына көшіріп, «General.txt» файлын сақтап көріңіз. Ақпараттың құпиялылық деңгейін төмендету әрекетіне байланысты қол жеткізуге тыйым салынады. «General.txt» файлын құпия «test» каталогына сақтаңыз.
Операциялық жүйенің кез келген параметрін өзгертіңіз (мысалы, «Қауіпсіздік» қойындысын көрсету: «Басқару тақтасы - Қалта параметрлері» бөліміндегі «Қарапайым файлды ортақ пайдалану» опциясын өзгерту). Қалта параметрлері қойындысын қайта іске қосыңыз және параметрдің күйін тексеріңіз. Outlook бағдарламасын іске қосып көріңіз. Амалдық жүйе мен қолданба параметрлеріне жасалған өзгертулер жалпы файлдарға жазылады және сақталмайды.
Осылайша, егер ағынды басқару қосылса, сеанс деңгейі файлдың құпиялылық деңгейіне тең болса, ақпаратты сезімталдық деңгейі төмен файлдарға көшіруден басқа барлық әрекеттерге рұқсат етіледі.
"D:\temp\Conf.txt" файлын алынбалы құралға көшіріп көріңіз. Көшіру сәтсіз болады, себебі бұл пайдаланушыға құпия ақпаратты алынбалы тасымалдағышқа көшіру құқығы берілмеді.

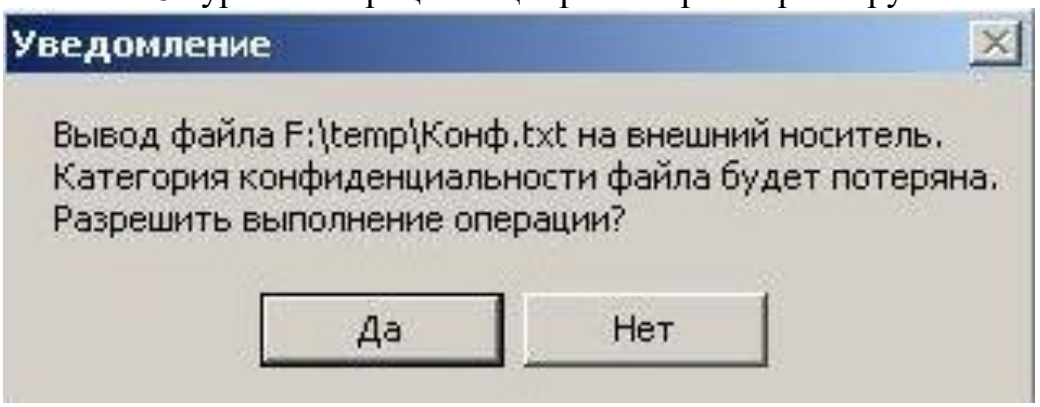
4.4. «Қоғамдық» сессия деңгейінде жұмыс
«Құпия» тіркелгімен кіріп, «Қоғамдық» сеанс деңгейін таңдаңыз.
"D:\temp\Conf.txt" файлын ашып, жойып көріңіз, оны жалпыға қолжетімді каталогқа (мысалы, "Жұмыс үстелі") және алынбалы құралға көшіріңіз. Сеанс деңгейі «Жария» болғанда, құпия ақпаратқа кез келген қол жеткізуге тыйым салынады. Бұл ретте жалпыға ортақ ақпаратқа қол жеткізу шектеусіз: Outlook бағдарламасын іске қосыңыз, жалпы файлды алынбалы тасымалдағышқа көшіріңіз.
Осылайша, деректер ағынын басқаруға негізделген тәсілдің арқасында құпия ақпараттың ағып кету мүмкіндігі алынып тасталады.

4.5. Құпия файлдарды алынбалы құралға көшіру
«Құпия» тіркелгімен кіріңіз. Жүйеге бірінші рет кірген кезде операциялық жүйені конфигурациялау қажет, ол тек «Қоғамдық» сеанс арқылы мүмкін болады, сондықтан құпия ақпаратқа қол жеткізуге тыйым салынады (Сурет 16).
Сеанстан шығып, Құпия сеанс деңгейін таңдап, Құпия тіркелгімен қайта кіріңіз.
"D:\temp\Conf.txt" файлын алынбалы құралға көшіріңіз. Көшіру кезінде файлдың

құпиялылық деңгейін жоғалтуы туралы ескерту пайда болады (Сурет 17). Құпиялықты жоғалтқанына қарамастан, көшіруге рұқсат етіледі, өйткені. пайдаланушыға алынбалы тасымалдағышқа құпия ақпараттың шығуы қамтамасыз етілді (4-сурет).



16-сурет - Операциялық жүйеге бірінші рет кіру



17-сурет - алынбалы құралға көшіру кезінде файлдың құпиялылықты жоғалтуы туралы ескерту

Жаттығу

1. Кестеге сәйкес. 1 Әкімші ретінде каталогтарды (D:\ дискінің түбірінде орналасқан) құпиялылық санаттарына тағайындаңыз.
2. Әрбір каталогта рұқсаты каталогтың құпиялылық санатына сәйкес келетін пайдаланушы атынан 2-4 құжат жасаңыз.
3. Құрылған құжаттарға қол жеткізу мүмкіндігін тексеріңіз.

Кесте

Тапсырма нұсқалары каталог және оның құпиялылық санаты қолжетімді

1	D:\БД\Заказы	D:\Договоры\ Спонсоры конфиденциально	D:\БД\Поставщики
2	D:\Договоры\Инвесторы секретно	D:\БД\Клиенты	D:\Договоры\ Партнёры
3	D:\Документация\Отчёты	D:\Документация\ Приёмные документы	D:\Документация\ Информация о сотрудниках
4	D:\Подразделения\Отдел сбыта	D:\Подразделения\ Отдел кадров	D:\Подразделения \Финансовый отдел
5	D:\Файлы\ Пользователи	D:\БД\ Поставщики	D:\Договоры\ Партнёры

6	D:\Файлы\Опытные пользователи	D:\БД\Заказы	D:\Договоры\ Спонсоры
7	D:\Файлы\Администраторы	D:\БД\Клиенты	D:\Договоры\ Инвесторы
8	D:\Подразде- ления\Отдел кадров	D:\Подразделения\ Финансовый отдел	D:\Подразделения \Отдел сбыта
9	D:\Файлы\ Опытные пользователи	D:\Файлы\ Пользователи	D:\Файлы\ Администраторы
10	D:\Документация \Приёмные документы	D:\Документация\ Отчёты	D:\Документация\ Информация о сотрудниках

Тест сұрақтары

1. Қол жеткізуді міндетті басқару механизмінің жұмыс істеу принципі неге негізделген?
2.Пайдаланушының рұқсат деңгейі файлдың құпиялылық санатынан жоғары болса, пайдаланушыға файлға кіру рұқсаты бар ма?
3. «Құпия ақпаратты шығару» функциясы нені білдіреді?
4. Әдепкі құпиялылық санаттарын тізімдеңіз.
5. Қандай опция құпиялылық санаттарын басқару мүмкіндігін береді?
6. FAT32 файлдық жүйесі бар дискіде орналасқан ресурсқа құпиялылық санатын тағайындауға бола ма?
7. «Жаңа файлдарды автоматты түрде тағайындау» опциясын түсіндіріңіз.
8. Деректер ағынын басқару не үшін қажет?
9.Қандай сеанс деңгейінде пайдаланушы операциялық жүйе мен қолданба параметрлерін өзгерте алады?
10. Сеанс деңгейінен төмен деңгейі құпия ақпаратқа қол жеткізу кезінде пайдаланушыға қандай құқықтар беріледі?

ОЖҚ. Зертханалық жұмыс №12. Құрылғыларға қол жеткізуді саралау

Зертханалық жұмыстың мақсаты: DeviceLock бағдарламалық өнімі негізінде құрылғыларға кіруді басқару принциптерін практикалық зерттеу.

Зертханалық жұмыстың міндеттері:

1. DeviceLock басқару консолін конфигурациялау
2. Құрылғыларға қол жеткізуді саралау
3. Ақ тізімдегі құрылғылар
4. Құрылғыны пайдалануды тексеру
5. Көлеңкелі көшірме файлдары
6. Квест
7. Қауіпсіздік сұрақтары

Зертханалық жұмыстың мазмұны:

Бұл мақалада компьютерге немесе домен әкімшісіне диск жетектеріне, CD / DVD дискілеріне, басқа алынбалы құрылғыларға, WiFi және Bluetooth адаптерлеріне, сондай-ақ USB, FireWire, инфрақызыл, COM және LPT порттарына пайдаланушы қатынасын басқаруға мүмкіндік беретін қолданбалар талқыланады.

Қол жеткізуді басқару екі деңгейде орындалуы мүмкін: интерфейс (порт) деңгейі және тип деңгейі (алынбалы құрылғы, принтерлер, қатты дискілер және т.б.). Кейбір құрылғылар екі деңгейде, ал басқалары тек біреуінде тексеріледі: интерфейс (порт) деңгейінде немесе тип деңгейінде.

DeviceLock үш бөліктен тұрады:

- *агент (DeviceLock қызметі). Агент әрбір компьютерге орнатылады, автоматты түрде іске қосылады және клиенттік компьютердегі құрылғыларды қорғауды қамтамасыз етеді;*
- *сервер (DeviceLock Enterprise Server). Бұл көлеңкелі көшірме деректері мен аудит журналдарын орталықтан жинау және сақтау үшін пайдаланылатын қосымша қосымша құрамдас;*
- *басқару консольдері. Бұл жүйе әкімшісі агент орнатылған кез келген жүйені қашықтан басқару үшін пайдаланатын басқару интерфейсі.*

Қарастырылған утилиталар мен қосымшалар:

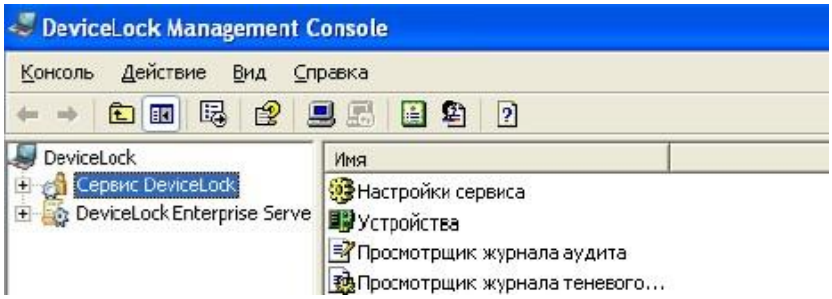
- *DeviceLock басқару консолі. Ол аудит рұқсаттары мен ережелерін көруге және өзгертуге, DeviceLock қызметін орнатуға және жеке компьютерлер үшін аудит пен көлеңке журналдарын көруге мүмкіндік береді.*

1. DeviceLock басқару консолін конфигурациялау

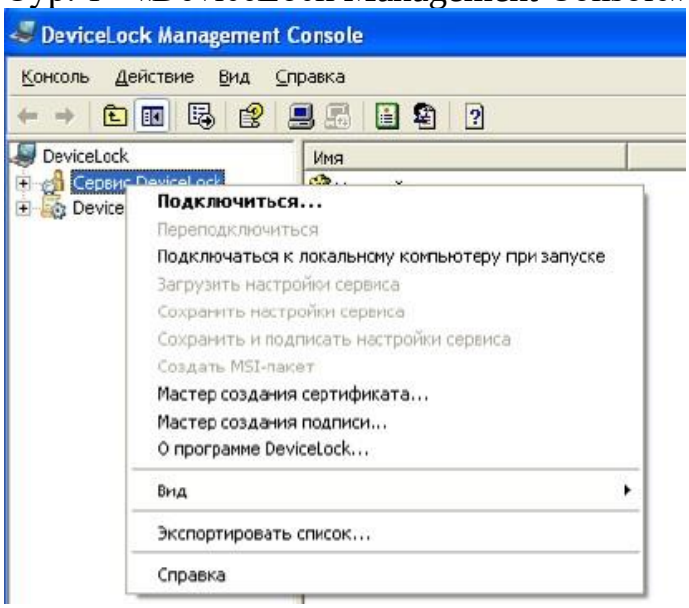
«Әкімші» тіркелгісі арқылы кіріңіз. «DeviceLock басқару консолін» іске қосыңыз: «Бастау - Бағдарламалар - DeviceLock» (Сурет 1). Сондай-ақ, консольге DeviceLock басқару консолінің қосымша модулін қосу арқылы MMC арқылы кіруге болады.

DeviceLock басқару консолін басқарылатын компьютерге қосыңыз. Мұны істеу үшін DeviceLock Service контекстік мәзірінде таңдаңыз

«Қосылу...» (Сурет 2). Сонымен қатар, қызметті автоматты түрде қосу үшін «Іске қосу кезінде жергілікті компьютерге қосылу» параметрін қосыңыз.

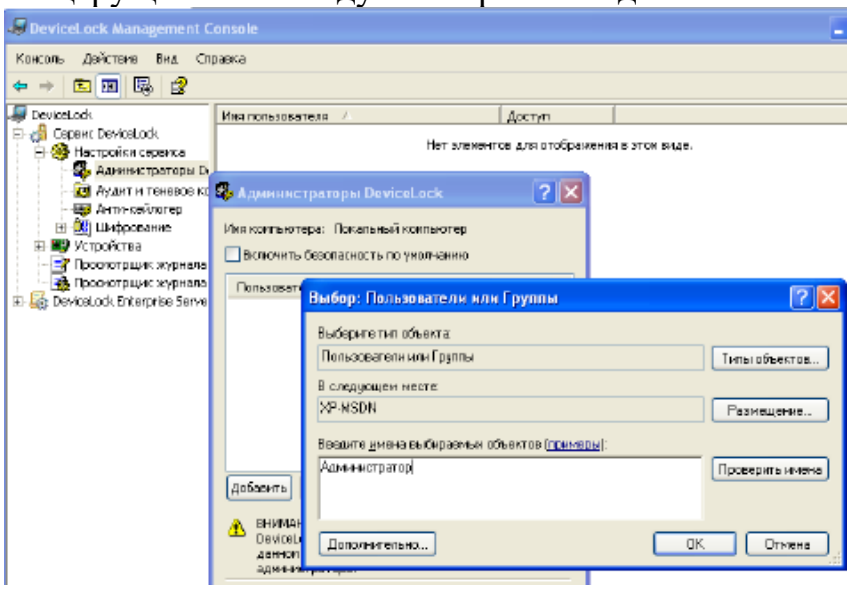


Сур. 1 - «DeviceLock Management Console»



Сур. 2 - DeviceLo консолін қосу

«Қызмет параметрлері - DeviceLock әкімшілері» қойындысына өтіңіз. DeviceLock әкімшісі ретінде «Әкімші» тіркелгісін қосыңыз (Сурет 3). Бұл қойындыда қосымша модульге кіруді шектеу мүмкіндігі бар басқа пайдаланушыларды қосуға болады (толық кіру, өзгерту, тек оқу). Тізімге қосылмаған пайдаланушылар құрылғыға кіруді басқару қосымша модуліне кіре алмайды.

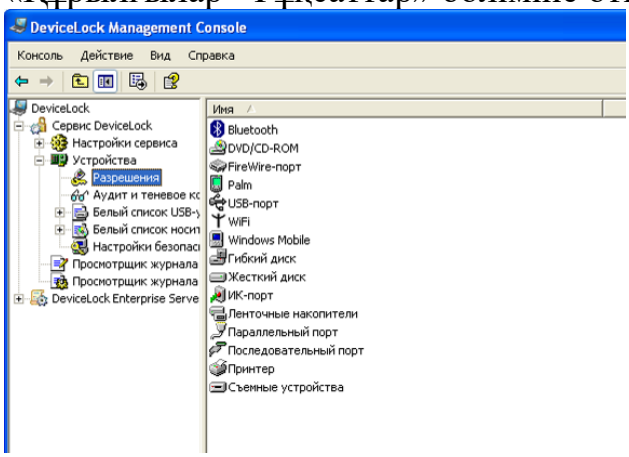


Сур. 3 - DeviceLock әкімшісін қосу

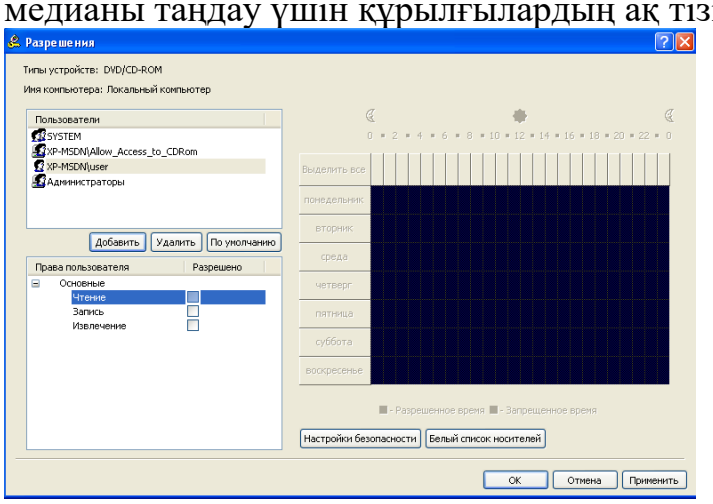
2. Құрылғыларға қол жеткізуді саралау

Пайдаланушы құрылғыға кіруге әрекет жасағанда, DeviceLock сұрауды ОЖ ядросы деңгейінде ұстайды. Құрылғы түріне және қосылым интерфейсіне (мысалы, USB) байланысты DeviceLock сәйкес кіруді басқару тізімінде (ACL) пайдаланушы

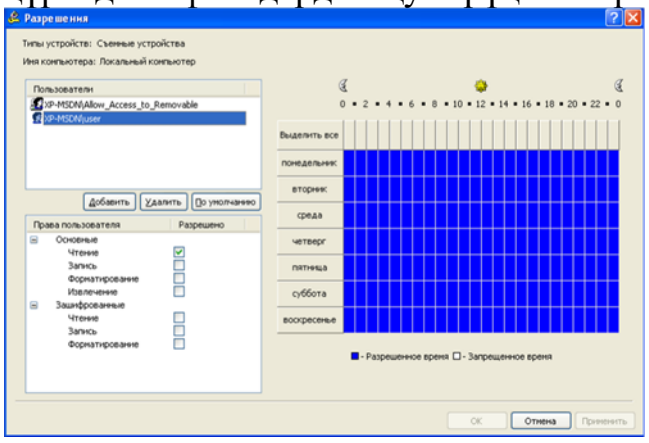
құқықтарын тексереді. Егер пайдаланушының осы құрылғыға кіру құқығы болмаса, қате туралы хабар қайтарылады - «кіру рұқсаты қабылданбады».
«Құрылғылар - Рұқсаттар» бөліміне өтіңіз (4-сурет)



Сур. 4 - Құрылғыларға арналған рұқсаттар
DVD/CD-ROM дискісіне «пайдаланушы» тіркелгісіне кіруге тыйым салу (Сурет 5). Егер компьютерде бірнеше CD / DVD дискілері орнатылған болса, белгілі бір медианы таңдау үшін құрылғылардың ақ тізімін пайдалануға болады.

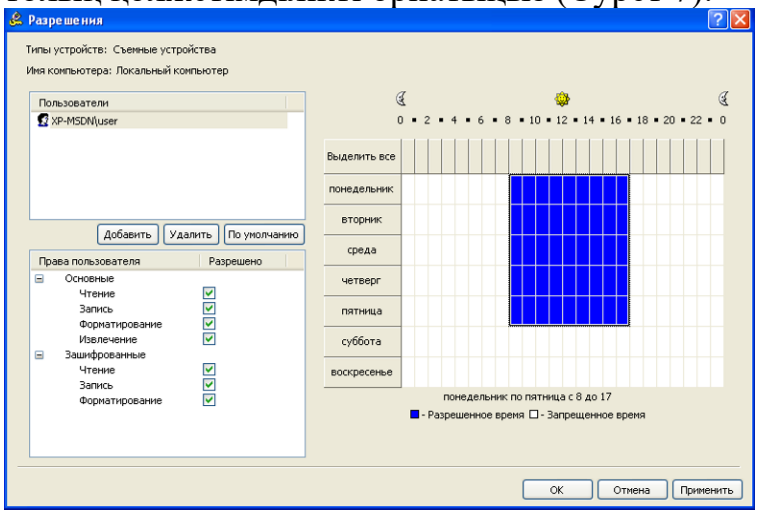


Сур. 5 - DVD/CD-ROM үшін рұқсаттар
«Пайдаланушы» тіркелгісімен кіріңіз. CD/DVD дискісіне қол жеткізу өшірілгеніне көз жеткізіңіз.
«Әкімші» тіркелгісі астында «пайдаланушы» пайдаланушыға тек алынбалы құралдағы файлдарды оқуға рұқсат беріңіз (Сурет 6).



Сур. 6 - алынбалы құрылғыларға арналған рұқсаттар

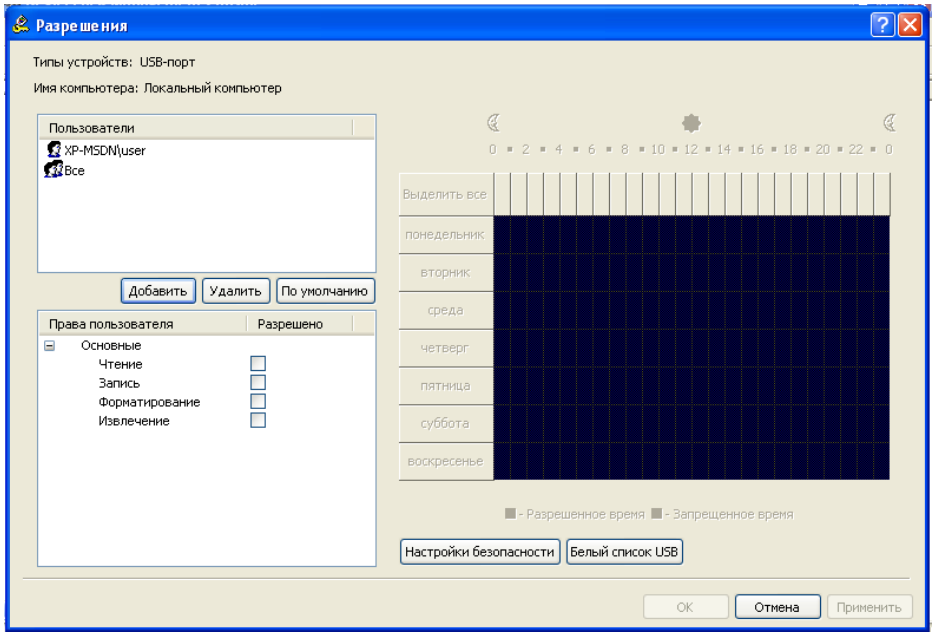
Ескертулер:
- егер пайдаланушы кез келген топтың мүшесі болса және бұл топтың құрылғыға толық рұқсаты болса, онда тек оқу режимі жұмыс істемейді (бұл рұқсаттардың жинақталуына байланысты);
- егер тіркелгі рұқсаттарға қосылмаса, оған кіруге тыйым салынады.
«Пайдаланушы» тіркелгісімен кіріңіз.
Алынбалы құралды қосып, оған жазу мүмкін емес екеніне көз жеткізіңіз.
DeviceLock аптаның күні және тәулік уақыты бойынша құрылғыларға кіруді шектеу мүмкіндігін береді.
«Әкімші» тіркелгісі арқылы жүйеге кіріп, «пайдаланушы» пайдаланушыға жұмыс күндері сағат 8:00-ден 17:00-ге дейін немесе сабақ кезінде алынбалы құрылғыларға толық қолжетімділікті орнатыңыз (Сурет 7).



Сур. 7 - Апта күні және тәулік уақыты бойынша құрылғыларға қол жеткізуді саралау
«Пайдаланушы» тіркелгісімен кіріңіз
Алынбалы құралды қосып, көз жеткізіңіз
оған қол жеткізуге рұқсат етілген.
Әкімші тіркелгісі астында жүйе уақытын жексенбіге өзгертіңіз.
«Пайдаланушы» тіркелгісімен жүйеге кіріп, алынбалы медиаға қол жеткізуге шектеуді тексеріңіз.

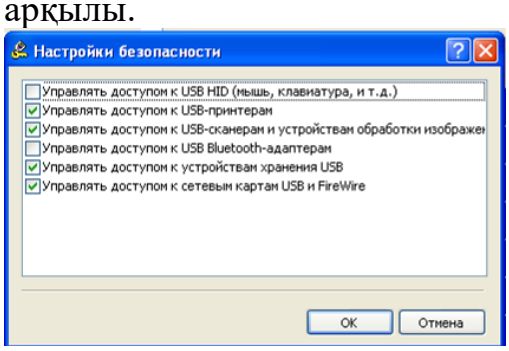
3. Құрылғылардың АҚ тізімі

"Әкімші" есептік жазбасының астында "пайдаланушы" есептік жазбасының USB портына кіруге тыйым салыңыз (сурет. 8).
USB құрылғылары жағдайында DeviceLock ең алдымен интерфейс деңгейіндегі рұқсаттарды тексереді (USB порты), USB портына кіру ашық немесе жоқ. Содан кейін, өйткені "Windows" USB флэшін алынбалы құрылғы ретінде анықтайды, DeviceLock сонымен қатар құрылғы түрінің (алынбалы құрылғы) деңгейіндегі шектеулерді тексереді. Есептік жазба астында "пайдаланушы" алынбалы медиаға кіруге тыйым салуды тексеріңіз.



Сурет. 8-USB портына арналған рұқсаттар

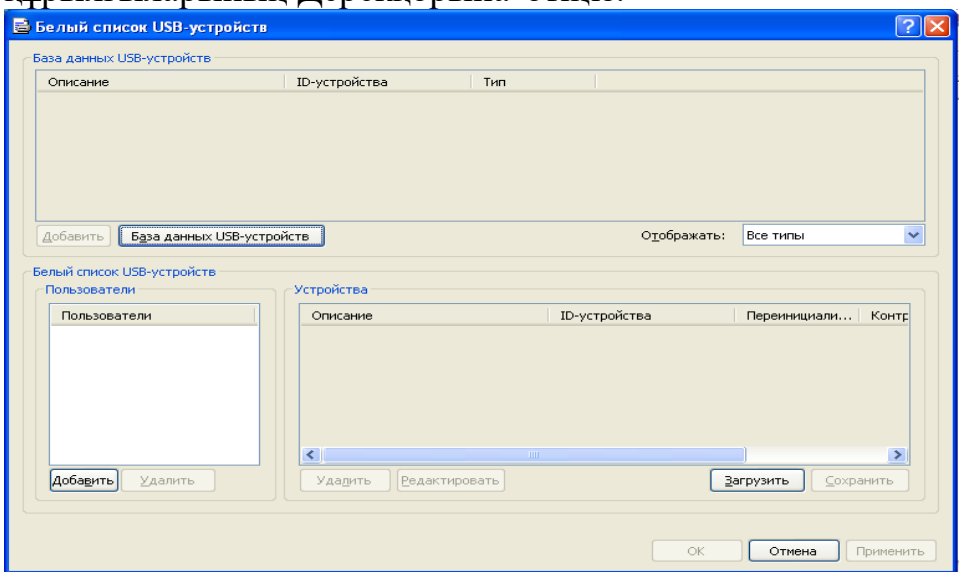
Барлық USB құрылғылары қол жетімділікті шектеуге ұшырағандықтан, ұйымда пайдалануға рұқсат етілген USB құрылғыларына ерекше жағдайлар жасау қажет.
Ерекшеліктерді екі жолмен көрсетуге болады:
- "қауіпсіздік параметрлері" арқылы (сурет. 9);
- модельді немесе құрылғының белгілі бір данасын анықтауға негізделген "ақ тізім" арқылы.



Сурет. 9-Қауіпсіздік параметрлері

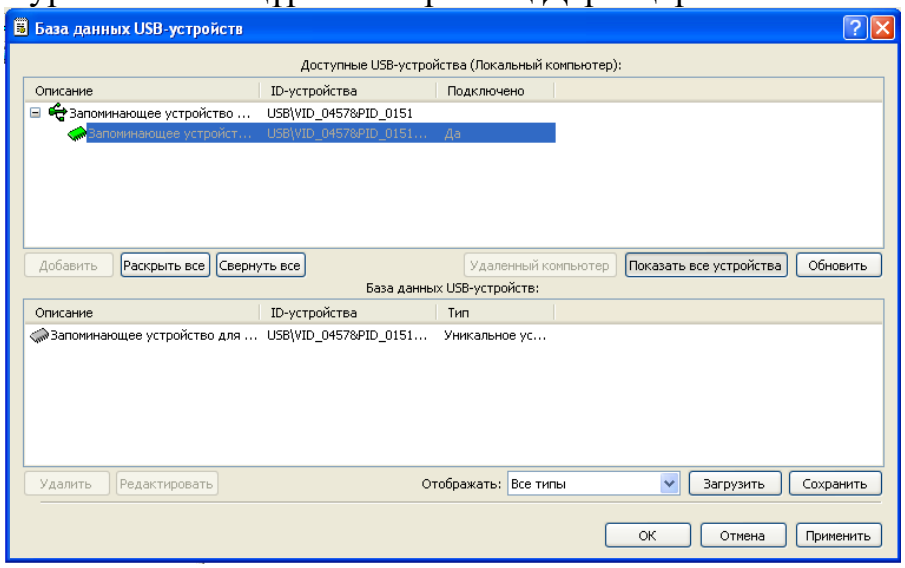
Егер "қауіпсіздік параметрлері" құрылғының кез-келген класын басқару параметрлерін қосса, онда осы кластағы құрылғыларға кіру демаркациясы қолданылады. Егер параметр өшірілген болса, онда барлық пайдаланушылар осы сыныптағы құрылғыларды қолдана алады.
Ақ тізімді пайдаланған кезде құрылғыны анықтаудың екі нұсқасы бар:
1) Device Model-бір модельдің барлық құрылғыларын сипаттайды. Әрбір құрылғы өндіруші идентификаторы (VID) және өнім (PID) комбинациясы арқылы анықталады. VID және PID тіркесімі белгілі бір құрылғыны емес, белгілі бір модельді сипаттайды. Бұл дегеніміз, осы өндірушінің осы моделінің барлық құрылғылары бір құрылғы ретінде танылады.
2) Unique Device-нақты бірегей құрылғыны сипаттайды. Әрбір құрылғы өндіруші идентификаторының (VID), өнімнің (PID) және сериялық нөмірдің тіркесімі арқылы анықталады.
Құрылғы ақ тізімге бірегей құрылғы ретінде қосылуы мүмкін, егер өндіруші оған

өндіріс кезеңінде сериялық нөмір берген болса.
Құрылғы ақ тізім арқылы рұқсат етілмес бұрын, ол дерекқорға қосылуы керек. "Құрылғылар - ақ USB тізімі" қойындысына өтіп, контекстік мәзірден "басқару"тармағын таңдаңыз. Пайда болған терезеде (сурет. 10) "USB құрылғыларының Дерекқорына"өтіңіз.

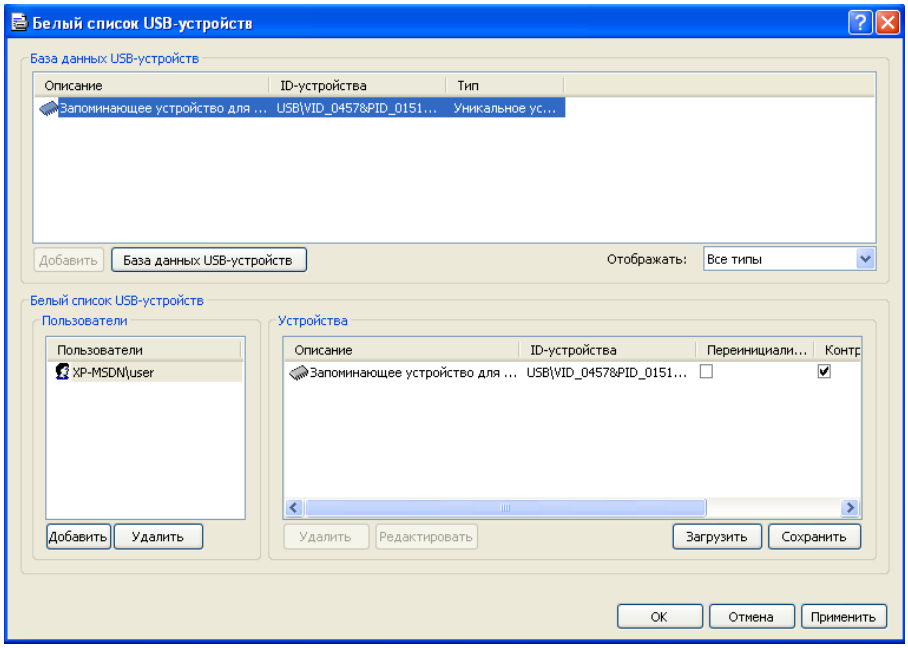


Сурет. 10-USB құрылғыларының АҚ тізімі

Құрылғыны таңдап, Қосу түймесін басу арқылы қол жеткізуге рұқсат беру керек USB құрылғыларын "құрылғы дерекқорына" қосыңыз (сурет. 11).
Сурет. 11-USB құрылғыларының Дерекқоры



"Пайдаланушы" пайдаланушысына USB құрылғысына дерекқордан кіруге рұқсат беріңіз. Ол үшін "пайдаланушы" есептік жазбасын қосып, "USB құрылғыларының дерекқорынан" қажетті құрылғыларды таңдаңыз (сурет. 12).



Сурет. 12 - құрылғыны пайдаланушының ақ тізіміне қосу

4. Құрылғыларды пайдалану аудиті

Қол жеткізуді басқару функциясынан басқа, DeviceLock пайдаланушылардың жергілікті компьютерде құрылғыларды пайдалануына хаттама жасауға және аудит жүргізуге мүмкіндік береді.

Пайдаланушының әрекеттерін хаттамалауды қосу үшін тиісті аудиторлық құқықтарды орнату қажет.

1) оқу/жазу - пайдаланушының деректерді оқу/жазу әрекеттері хаттамаланады. Құрылғы түрлері үшін "Bluetooth, FireWire порты, IR порты, параллель порт, сериялық порт, USB порты және WiFi".

2) Басып шығару - пайдаланушының құжаттарды принтерлерге жіберу әрекеттері хаттамаланады. Тек "Принтер"түріне қолданылады.

3) орындау - пайдаланушының құрылғы жағындағы кодты қашықтан орындау әрекеттері хаттамаланады. Тек "Windows Mobile"түріне қолданылады.

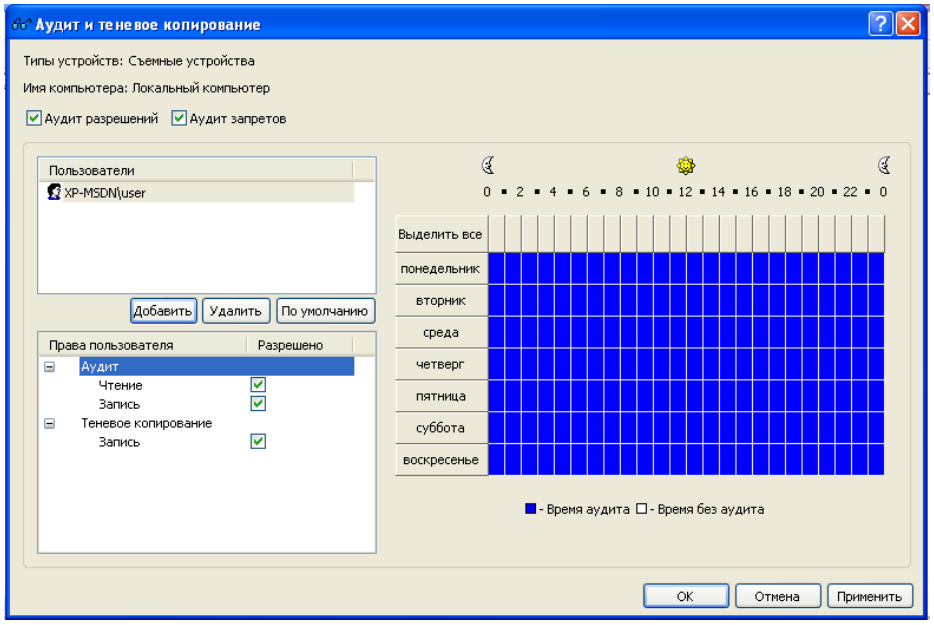
4) файлдарды оқу/жазу-пайдаланушының файлдық емес объектілерді (күнтізбе, контактілер, тапсырмалар және т.б.) оқу/жазу әрекеттері хаттамаланады. Тек "Windows Mobile" және "Palm"түрлеріне қолданылады.

Құрылғыларға сәтті қол жетімділік пен кіру қателерін тіркеу мүмкіндігі бар:

1)" рұқсат аудиті " - DeviceLock рұқсат берген барлық кіру әрекеттері, яғни пайдаланушыға құрылғыға кіру мүмкіндігі берілді.

2)" тыйым салу аудиті " - DeviceLock бұғаттаған барлық кіру әрекеттері, яғни пайдаланушыға құрылғыға кіруге тыйым салынды.

"Құрылғылар-Аудит және көлеңкелі көшіру" бөліміне өтіңіз. Алынбалы құрылғыларға "user" пайдаланушысы үшін аудитті қолданыңыз (сурет. 13).



Сурет. 13-алынбалы құрылғылар үшін аудитті орнату

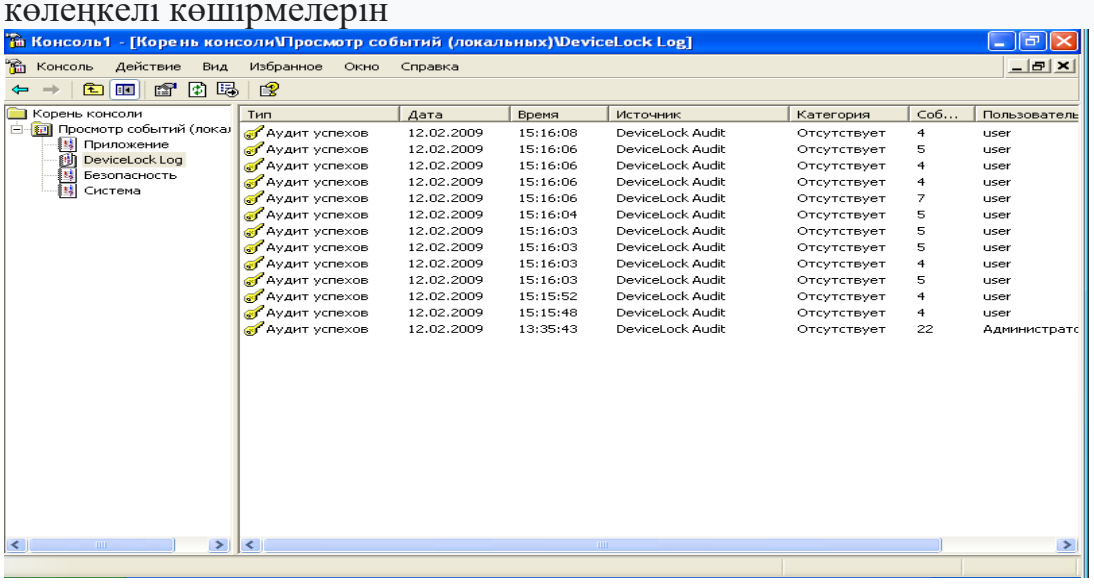
Канатбекова Асем 9-12

Сурет 16 - Құрылғы құлпы журналы қойындысы

5. Көлеңкелі көшірме файлдары

Көлеңкелі көшірме пайдаланушы алынбалы құралға көшіретін немесе басып шығаруға жіберетін барлық файлдардың көшірмелерін сақтауға мүмкіндік береді. Сақталған файлдарды құпия ақпарат үшін қосымша талдауға болады.

DeviceLock бөліміне өтіңіз «Құрылғылар - Аудит және көлеңкелі көшірме». «Пайдаланушы» пайдаланушысы үшін алынбалы құрылғылардағы файлдардың көлеңкелі көшірмелерін

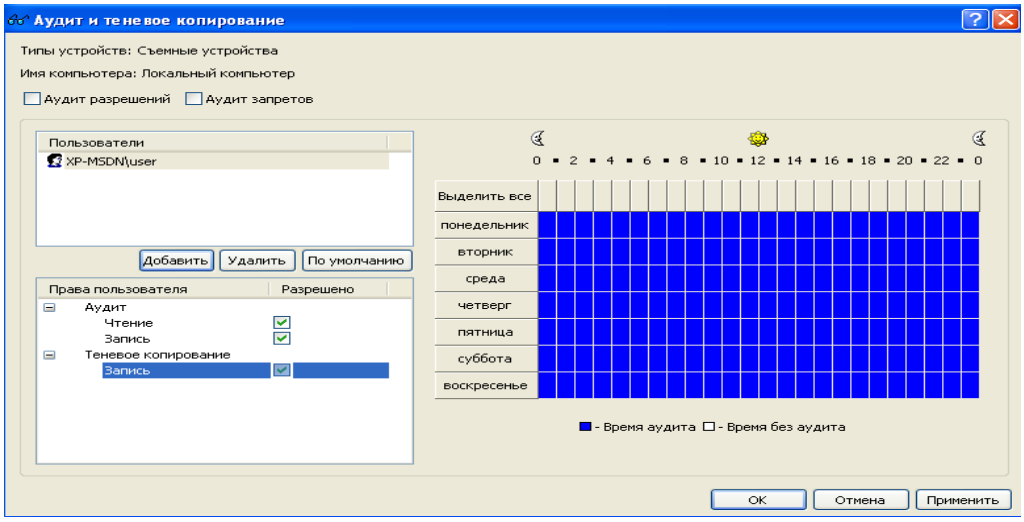


Сурет 17 - алынбалы құрылғылар үшін көлеңкелі көшірмені қосыңыз

«Пайдаланушы» тіркелгісі астында алынбалы құрылғыны қосыңыз және оған мәтіндік немесе графикалық файлды көшіріңіз.

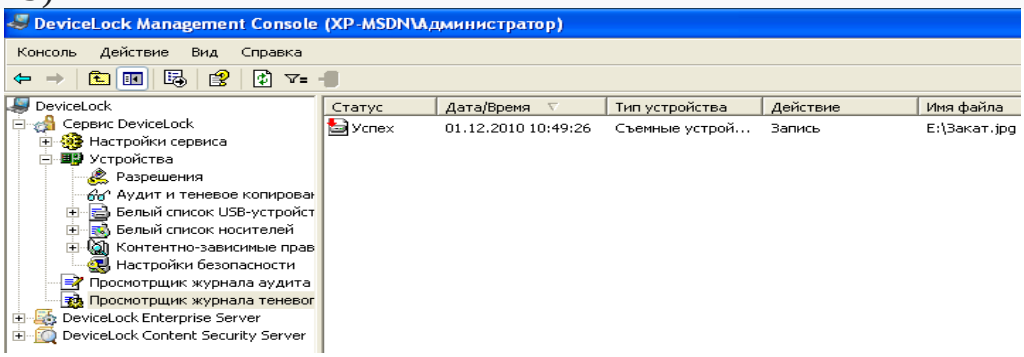
«Әкімші» тіркелгісі астында DeviceLock бөлімін ашыңыз

«Көлеңке журналын қарау құралы» (Сурет 18).



8 - Көлеңке журналын қарау құралы

Пайда болған журнал жазбасын ашыңыз. Бұл пайдаланушы «пайдаланушы» алынбалы құрылғыға көшірген файлдың мазмұнын көруге мүмкіндік береді.
Файлдардың көлеңкелі көшірмелерін сақтау орнын таңдау «Қызмет параметрлері - Аудит және көлеңкелі көшіру - Жергілікті каталог» бөлімінде мүмкін болады (Сурет 19)



Жаттығу
«Пайдаланушы» тіркелгісі үшін рұқсаттарды сәйкесінше орнатыңыз.
1 нұсқа

DVD/CD-ROM	Принтер	Қатты диск
Тек оқу. Ақ түске бір тасымалдаушы қосыңыз тізім. Виртуалды дискілерге толық қол жеткізу	Жұмыс күндері қол жеткізу. Аудитті басып шығару және кіруге тыйым салу	Толық қолжетімділік. Аудитті оқу және жазу

2 Нұсқа

Алынбалы құрылғылар	USB-порт	WIFI
Оқу және шығару	Барлық оқиғалардың аудиті	Жұмыс күндері қол жеткізу

Нұсқа 3

Алынбалы құрылғылар	USB-порт	DVD/CD-ROM
Оқу және шығару	Сканерлерге, принтерлерге, USB сақтау құрылғыларына қол жеткізуге тыйым салу. 3 қосыңыз ақ тізімге енгізілген құрылғылар	бастап жұмыс күндері ғана қол жеткізу 17-19 сағат. Жазба және рұқсаттардың аудиті

Нұсқа 4

WindowsMobile	Алынбалы құрылғылар	USB-порт
Тек оқу. Барлық оқиғалардың аудиті	Жұмыс уақытынан тыс уақытта кіруге тыйым салу	Тек оқу. 2 құрылғыны ақ тізімге қосыңыз

Нұсқа 5

Параллель порт	Жёсткий диск	Алынбалы құрылғылар
Рұқсат жоқ.	Жұмыс күндері 8-ден 20-ға дейін қол жеткізу сағат	Оқу және шығару. Аудит барлық оқиғалар.

Нұсқа7

Сериялық порт	USB-порт	Принтер
Жұмыс уақытынан тыс уақытта кіруге тыйым салу. арқылы қосылған модемдерге қол жеткізу берілген порт, шектеулер жоқ.	Рұқсат жоқ. Ақ тізімге 4 құрылғы қосыңыз	Таңғы 8-ден кешкі 6-ға дейін кіру. Барлық оқиғалардың аудиті.

Нұсқа8

Bluetooth	Параллельный порт	WindowsMobile
Шектеусіз қол жеткізу.	Жұмыс күндері қол жеткізу.	Шектеусіз қол жеткізу. Аудитті тіркеу.

Нұсқа 9

DVD/CD-ROM	USB-порт	Жёсткий диск
Тек оқу.	Оқу, шығару	Барлық оқиғалардың аудиті.
	Добавить в белый список 3 устройства.	

Нұсқа 10

FireWire-порт	WIFI	Алынбалы құрылғылар
Тек оқу. Аудит жазбалар мен тыйымдар	Жұмыс уақытында қол жеткізу. Аудитті оқу және жазу.	Рұқсат жоқ. Аудит тыйымдар

Тест сұрақтары
1. DeviceLock қолданбасының басқаруына кіруді шектеу мүмкін бе?
2. Интерфейс деңгейі мен құрылғы типі деңгейінің айырмашылығы неде?
3. DeviceLock қандай ресурстарға қол жеткізуді басқару функцияларын қамтамасыз етеді?
4. USB құрылғыларының сыныптарын (мысалы, тышқандар, пернетақталар және т.б.) қол жеткізуді басқару механизмінен қалай шығаруға болады?
5. Ақ тізімдер не үшін пайдаланылады?
6. Қандай құрылғылар кластарын ақ тізімге енгізуге болады?
7. Ақ тізімде құрылғыны анықтаудың қандай опциялары қолданылады?
8. Құрылғының деректер базасы не үшін қолданылады?
9. Құрылғыны тексеру журналдарын қайда сақтауға болады?
10. Файлдың көлеңкелі көшірмесі не үшін қолданылады?

Жаттығу
Зертханалық есеп нұсқаулықта сипатталған стандартқа сәйкес орындалады

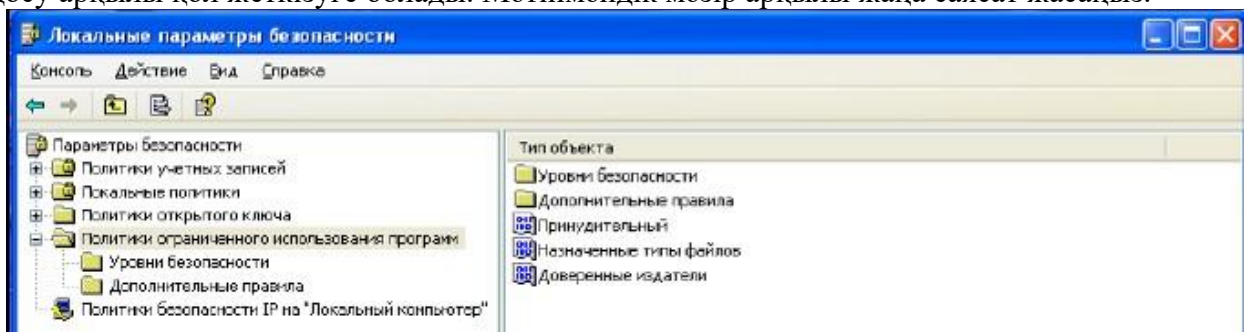
ОЖҚ. Зертханалық жұмыс № 13. БАҒДАРЛАМАЛАРДЫ ШЕКТЕУЛІ ПАЙДАЛАНУ

Зертханалық жұмыстың мақсаты: Windows ОЖ-де бағдарламаларды пайдалануды шектеудің кіріктірілген құралдарымен танысу және практикалық қолдану.

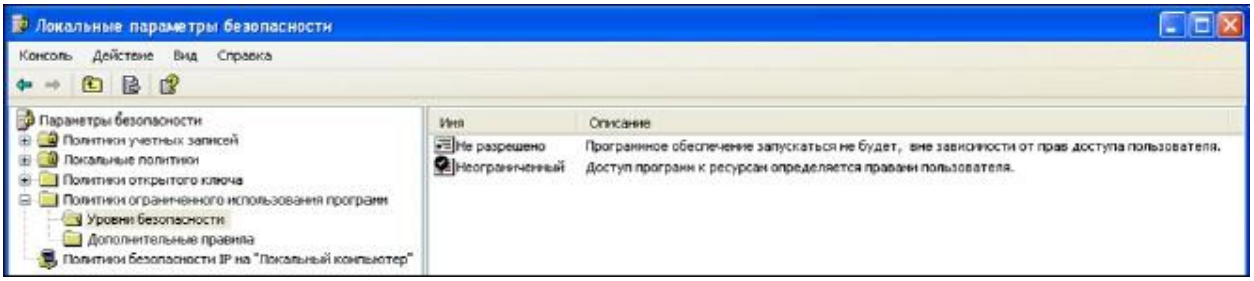
Зертханалық жұмыстың міндеттері:
1. Жұмыс барысы тапсырма
Бақылау сұрақтары

Зертханалық жұмыстың мазмұны:
Бағдарламаларды шектеулі пайдалану саясаты Windows отбасының ОЖ-де жұмыс істейтін бағдарламаларды анықтауға және оларды жергілікті компьютерде орындау мүмкіндігін басқаруға мүмкіндік береді.
Бағдарламаларды шектеулі пайдалану саясаты (POIP) - бұл әкімшілерге бағдарламалық қосымшаларға рұқсат беруге немесе тыйым салуға мүмкіндік беретін қауіпсіздік саясатының бір түрі. Қолдану файлды хэштеу алгоритмін қолдануға, файл жолдарын бағдарламалық жасақтамамен байланыстыруға, бағдарламалық жасақтама шығарушының сертификатына немесе бағдарламалық жасақтама жұмыс істейтін интернет аймағына негізделген.

1. Жұмыс барысы
1.Әкімші тіркелгісінің астындағы ОЖ-ге кіріп, келесі жолға өтіңіз: "Басқару тақтасы - әкімшілік - жергілікті қауіпсіздік саясаты", содан кейін консоль ағашында "бағдарламаларды шектеулі пайдалану саясаты" түйінін ашыңыз (сурет. 1). Сондай-ақ, бағдарламаларды шектеулі пайдалану саясатына (бұдан әрі-ПОИП) басқару консоліне "жергілікті қауіпсіздік параметрлері" жабдығын қосу арқылы қол жеткізуге болады. Мәтінмәндік мәзір арқылы жаңа саясат жасаңыз.



1-сурет.Жергілікті қауіпсіздік параметрлері

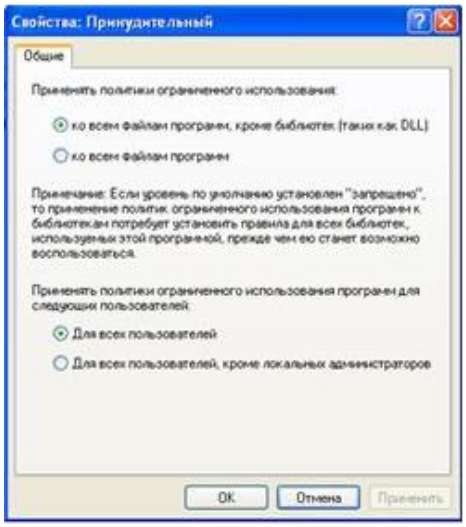


2-сурет.Қауіпсіздік деңгейін таңдау

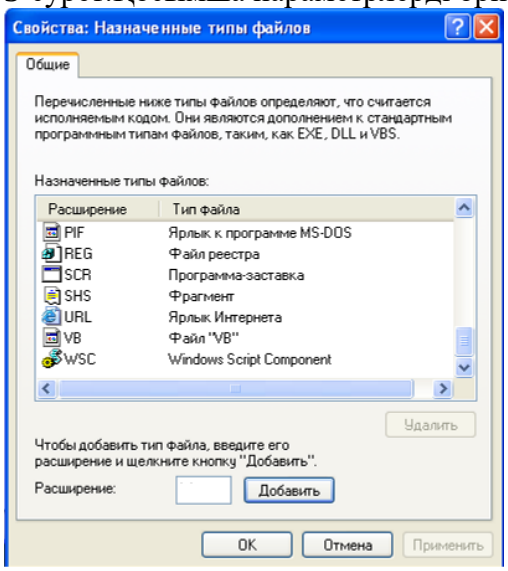
2."Қауіпсіздік деңгейлері" нысанын ашыңыз (сурет. 2) оған екі деңгей кіреді:
"Рұқсат етілмейді", ПОИП-қа рұқсат етілгеннен басқа кез келген БҚ-ны іске қосуға тыйым салуды және құқықтарға сәйкес БҚ-мен жұмыс істеу мүмкіндігін білдіретін" шектеусіз " дегенді білдіреді пайдаланушы. Әдепкі деңгей оны өзгерту үшін "О" деп белгіленеді қауіпсіздік деңгейін екі рет нұқыңыз және "әдепкі"тармағын таңдаңыз. Әдепкі қауіпсіздік деңгейі ретінде "шексіз" деңгейін орнатыңыз.
3.ПОИПТІ жергілікті әкімшілерге қолдану үшін "мәжбүрлі" нысан түрін екі рет нұқыңыз және "барлық пайдаланушылар үшін" таңдаңыз (сурет. 3). Мұнда басқа рұқсат етілген бағдарламалар

қолдана алатын DLL сияқты бағдарламалардың кітапханаларына POIP қолдануды болдырмау мүмкіндігі конфигурацияланған. ПОИП қолданбасын барлық пайдаланушылар мен файлдарға орнатыңыз.

4."Бағдарламаларды шектеулі пайдалану саясаты "бөлімінің" тағайындалған файл түрлері " тармағында барлық ережелер үшін пайдаланылатын тағайындалған файл түрлерінің тізімі бар. ПОИП қандай файл түрлерімен жұмыс істейтінін анықтау үшін пайда болған терезеде "тағайындалған файл түрлері" тармағын таңдаңыз (4-сурет.) өрісте "Кеңейтім: "қажетті кеңейтімді енгізіңіз, мысалы,"exe". Осылайша, жол ережесінде ескерілетін файлдардың жаңа түрлері қосылады.

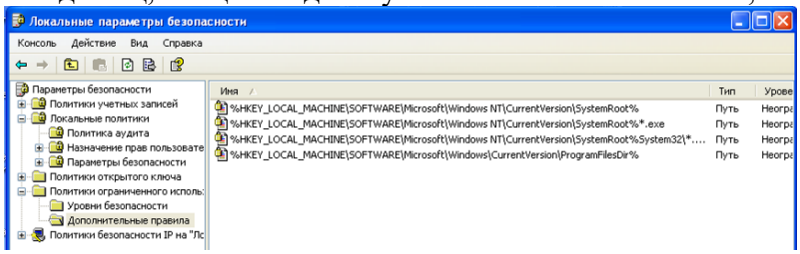


3-сурет.Қосымша параметрлерді орнату



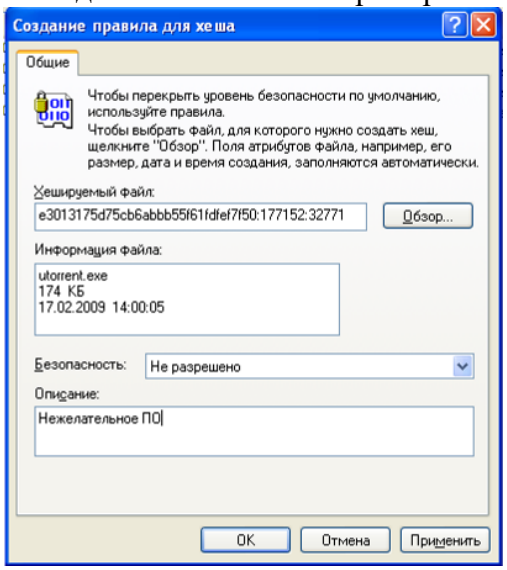
4-сурет. ПИОП бойынша файл түрлерінің тізімі

5."Қосымша ережелер" тармағына өтіңіз (5-сурет.) онда төрт жол ережесі бар. Олар ОЖ-ны әдепкі бойынша таңдалған қауіпсіздік деңгейінде "рұқсат етілмейді"іске қосуды қамтамасыз етеді. Мәзірден "әрекет" тармағын таңдаңыз, содан кейін "хэш ережесін жасаңыз...", пайда болған терезеде (6-сурет.) "Шолу" батырмасын пайдаланып, жұмыс істеуге тыйым салғыңыз келетін файлды көрсетіңіз, мысалы, "utorrent.exe", ол туралы ақпарат автоматты түрде толтырылады. Сондай-ақ, басқа пайдаланушы есептеген хэш мәнін, мысалы, вирустың хэшін енгізуге болады.

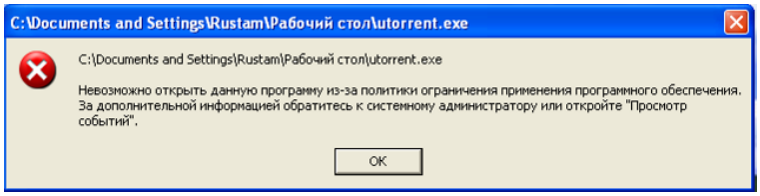


5-сурет.Қосымша ережелер қойындысы

"Utorrent" файлын іске қосыңыз.exe", содан кейін хабарлама көрсетіледі (7-сурет.) пайдаланушыға файлды іске қосуға тыйым салу туралы хабарлайды.
Файлдағы кез-келген өзгерістер хэштің өзгеруіне әкелетінін есте ұстаған жөн.



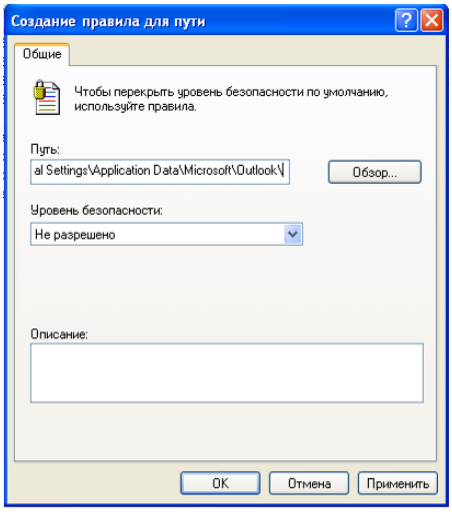
6-сурет.Хэш ережесін құру



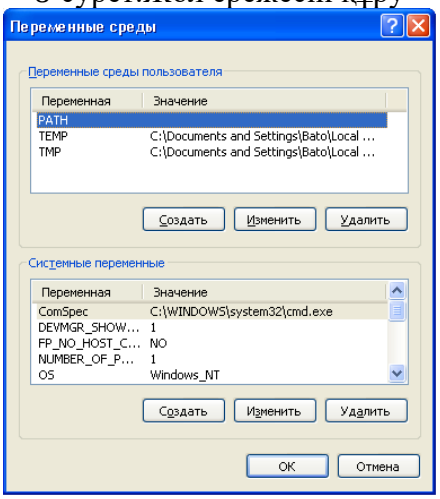
7-сурет.Ашуға тыйым салу туралы хабарлама

6.Хэш ережесіне ұқсас Жол ережесін жасаңыз. Пайда болған терезеде (8-сурет.) "жол:" өрісіне жұмыс істеу шектелуі керек файлдарға жолды енгізіңіз, мысалы:
"%programfiles%\messenger "және"рұқсат етілмеген" қауіпсіздік деңгейін таңдаңыз. Жолды белгілі бір файлға көрсетуге, сондай-ақ қойылмалы таңбаларды пайдалануға болады
"*"және"?", мысалы: "c:\downloads* .*».
"Windows Messenger" хабар алмасу бағдарламасын іске қосып көріңіз.
Іске қосылмағанына көз жеткізіңіз.

Жол ережесінде "%programfiles%", "%systemroot%"сияқты жүйелік айнымалыларды пайдалану мүмкіндігі бар, "%userproffle%"," %windir%"," %appdata% "және" %temp%", сондай-ақ қоршаған орта айнымалылары. Қоршаған ортаның айнымалылары жасалады келесідей: "Бастау - Басқару тақтасы - жүйе сипаттары" жолындағы жүйенің қасиеттерінде "қосымша" қойындысында "қоршаған орта айнымалылары" батырмасын басыңыз. Содан кейін пайда болған терезеде (9-сурет.) "Жасау"түймесін басыңыз. Айнымалы атауды енгізіңіз, мысалы, "бөлісу" және айнымалы мән "C:\Documents and Settings\All Users\құжаттар". Айнымалыны қолдану арқылы жол ережесін жасаңыз және тексеріңіз
«%Share%».

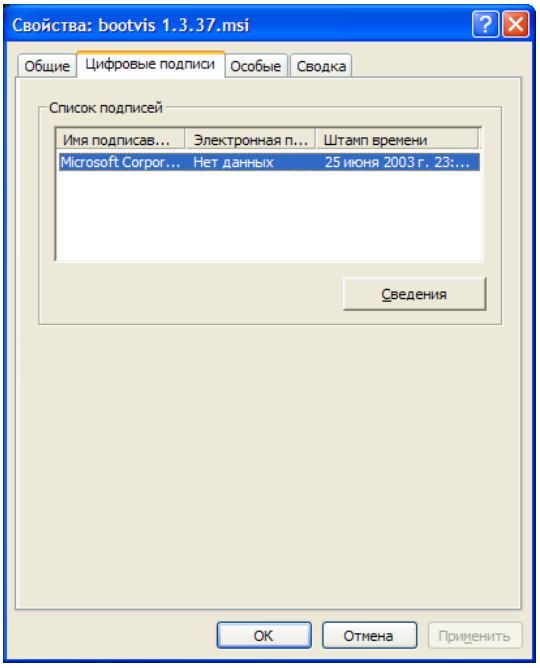


8-сурет.Жол ережесін құру



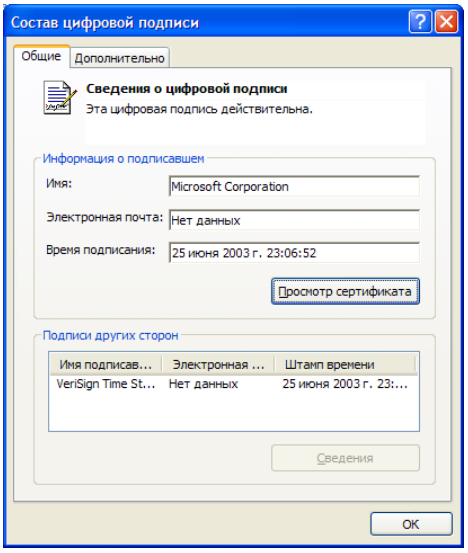
9-сурет.Қоршаған орта айнымалыларын құру

7."Интернет аймағына арналған ережелер..."олар тек Windows бағдарламалық жасақтамасын орнатушы пакеттеріне қолданылады, аймақтарды қосу қауіпсіздік қойындысындағы" Internet Explorer " шолғышының қасиеттерін қолдану арқылы жүзеге асырылады.
8үСертификат ережесін жасамас бұрын сертификатты келесідей алыңыз: мысалы, "bootvis.msi", қойынды "Сандық қолтаңбалар" (10-сурет.). Әрі қарай, пайда болған терезеде "мәліметтер" түймесін басыңыз (11-сурет.) "сертификатты қарау" түймесін басыңыз. Сертификат жарамды болуы керек. Пайда болған терезеде (12-сурет.) "композиция" қойындысын таңдап, "Файлға көшіру" түймесін басыңыз.", сертификаттарды экспорттау шеберінің көмегімен сертификатты сақтаңыз, мысалы, " Microsoft.cer " (сақтау форматы - X. 509).

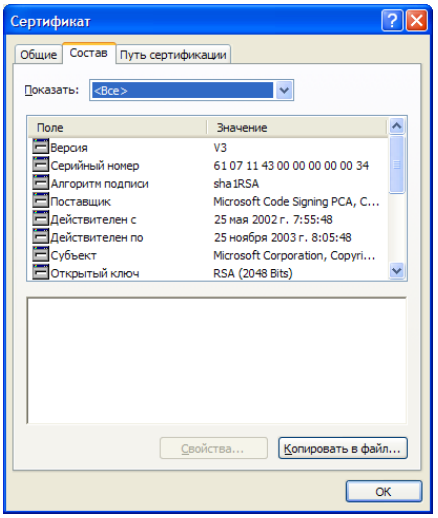


10-сурет. Сандық файл қолтаңбалары

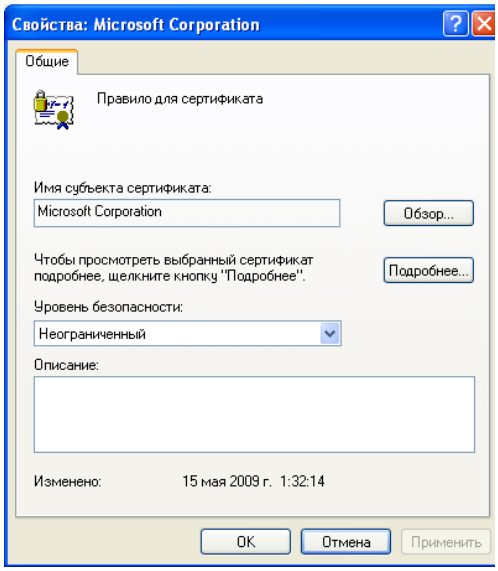
Әдепкі қауіпсіздік деңгейін "рұқсат етілмеген"етіп тағайындаңыз. Әрі қарай, қосымша ережелерде "сертификат ережесін" жасаңыз.", пайда болған терезеде (сурет. 13) сақталған сертификат файлының жолын көрсетіңіз "Microsoft.cer "және" шектеусіз " қауіпсіздік деңгейін орнатыңыз."Bootvis" файлын көшіріңіз.msi"қалтаға "C:\Documents and Settings\All Users\ құжаттар". Осы сертификатпен қол қойылған орнату пакетін іске қосуға тырысқанда, сертификат ережесінің жол ережесінен басымдығы орындалады. Іске қосу мүмкіндігін тексеріңіз. Сертификат ережесі қол қойылған бағдарламалардың портативті ақпарат құралдарынан іске қосылуын шектеуі мүмкін.



11-сурет. Файлдың сандық қолтаңбасының құрамы



12-сурет.Сертификат



13-сурет.Сертификатқа арналған ережелер терезесі

9. Бірнеше ережелерді қолдану кезінде туындайтын қақтығыстарды шешу үшін басымдық қолданылады. Төменде басымдықтың кему ретімен ережелер келтірілген.
1) хэш ережесі.
2) сертификатқа арналған ереже.
3) жол ережесі. Жол ережелерінің қайшылығы кезінде үлкен шектеулі ереже басымдыққа ие болады. Төменде ең жоғары басымдықтан (ең үлкен шектеу) ең төменгі басымдыққа дейінгі жолдар жиынтығы берілген.
- диск: \ қалта1\қалта2\Файл атауы.кеңейту
- диск: \қалта1 \қалта2\ * .кеңейту
- *.кеңейту
- диск: \ қалта1 \қалта2\
- диск: \ қалта1 \
4) интернет аймағына арналған ереже.

Жолға қатысты екі ұқсас ереже қақтығысқан кезде, үлкен шектеу ережесі басымдыққа ие болады. Мысалы, егер жол ережесі болса "C:\Windows\" қауіпсіздік деңгейімен "рұқсат етілмейді" және "%windir%" жолының ережесі
"Шектеусіз", қауіпсіздік деңгейімен қатаң ереже қолданылады
"Рұқсат етілмейді".
Мысал ретінде бағдарлама үшін рұқсат етілген хэш ережесін жасаңыз

«calc.тыйым салынған жол бойында орналасқан" exe "c:\downloads". Әрі қарай, бұл бағдарламаны бұрын тыйым салынған жолдан бастауға тырысыңыз. Хэш ережесінің басымдығы бағдарламаны осы қалтадан іске қосуға мүмкіндік береді.
Тапсырманы орындамас бұрын жасалған барлық ережелерді жойыңыз.
Тапсырма
Кесте 1. Тапсырмаларды нұсқалар бойынша бөлу

Нұсқа номері	***Тапсырма***
1	с а по д
2	с б по е
3	с в по ж
4	с г по з
5	с д по и
6	с е по к
7	с ж по л
й	с з по м
9	с к по о
10	с л по п

1. Келесі бағдарламаларды пайдалануды шектеу саясатын жасаңызболады сіздің нұсқаңызға сәйкес келесі талаптарды қанағаттандырыңыз (кесте. 1):
а)"Microsoft" сертификатымен қол қойылған бағдарламалық жасақтаманы іске қосуға мүмкіндік береді;
б) барлық пайдаланушыларға, соның ішінде жергілікті әкімшілерге қолданылады;
в) шектемейді "DLL"сияқты бағдарламалық кітапханаларды пайдалану;
г) сенімді баспагерлерді таңдау құқығы тек жергілікті әкімшілерге рұқсат етіледі:
д) кез-келген бағдарламаны әдепкі қауіпсіздік деңгейі ретінде іске қосуға тыйым салады;
е) кез-келген бағдарламаларды қалталардан іске қосуға мүмкіндік береді: "C:\WINDOWS", "C:\Program файлдар", «C:\Documents and Settings\LocalService», «C:\Documents and Settings\All Users»;
ж) кез-келген бағдарламаны іске қосуға мүмкіндік бередіқолданушыоның қалтасынан "C::documents and Settings user" (мұндағы user - кез келген пайдаланушының аты) айнымалы арқылы қоршаған орта:
з) Жол ережелерінің басымдығы арқылы пайдаланушыға кез келген бағдарламаны іске қосуға тыйым салынады басқа қалталар пайдаланушылар, мысалы, "Бірге: \ құжаттар және Параметрлер\әкімші";
и) "Microsoft" сертификатымен қол қойылған бағдарламалық жасақтаманы орнатуға рұқсат береді; туралы
k) өрмекші, Сапер және utorrent бағдарламаларын іске қосуға тыйым салады.exe " оларға қарамастан орналасқан жері;
л) "AUTORUN.INF " кез келген жерден;
м) жергілікті әкімшілерді қоспағанда, барлық пайдаланушыларға қолданылады;
н) "DLL" сияқты бағдарламалық кітапханаларды пайдалануды шектейді;
о) сенімді баспагерлерді таңдау құқығы кез келген пайдаланушыға рұқсат етіледі;
п) "Microsoft" сертификатымен қол қойылған бағдарламалық жасақтаманы орнатуға тыйым салады.
2. Стандартты "Explorer" Explorer және үшінші тарап көмегімен жасалған барлық ережелерді тексеріңіз файл менеджері, мысалы," Far manager "немесе" Total Commander", олар елемейді ме ПОИП?

Бақылау сұрақтары
1) бағдарламаларды шектеулі пайдалану саясатын қалай құруға болады?

2) ПОИП-тан жергілікті әкімшілер шығарылуы мүмкін бе?
3) "тағайындалған файл түрлері"тармағы не үшін қызмет етеді?
4) хэш ережесінің жол ережесінен басты артықшылығы неде?
5) хэш ережесімен тыйым салынған бағдарлама орындалуы мүмкін болған кезде мысал келтіріңіз.
6) Сертификат ережесі не үшін қолданылады?
7) файлдан сертификатты қалай алуға болады?
8) Ереженің басымдылығын пайдаланудың үш мысалын келтіріңіз.
9) кеңейтімі бар кез келген файлды ашуды қалай тоқтатуға болады".swf " қатты дискідегі кез келген жерден?
10) "шектеусіз" және "рұқсат етілмеген" қауіпсіздік деңгейлерінің арасындағы айырмашылықты түсіндіріңіз.

Тапсырма

Зертханалық жұмыс туралы есеп әдістемелік нұсқауларда сипатталған стандарт бойынша орындалады

ОЖҚ. Зертханалық жұмыс №14. Операциялық жүйе қауіпсіздік оқиғаларының аудиты

Зертханалық жұмыстың мақсаты: мысал ретінде Windows операциялық жүйесін пайдалану арқылы қауіпсіздік аудитінің ішкі жүйесінің басқару интерфейсімен және аудит саясатының параметрлерімен танысу.

Зертханалық жұмыстың міндеттері:

1. Аудит саясаты
2. Пайдаланушының кіру/шығуын тексеру
3. Әкімшілікпен байланысты оқиғаларды тексеру
4. Операциялық жүйенің жұмысына байланысты оқиғаларды тексеру
5. Пайдаланушының ресурстарға қол жеткізуін тексеру
6. Аудит журналын басқару тапсырмасы

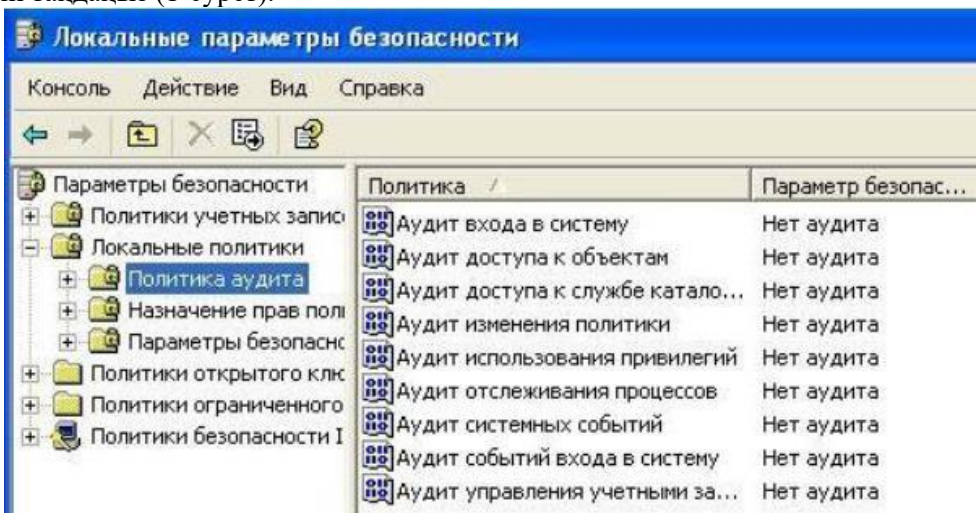
тест сұрақтары

Зертханалық жұмыстың мазмұны:

1. Аудит саясаты

Аудит саясаты оқиға хабарларының қай санаттары бақыланатынын және қауіпсіздік журналында сақталатынын анықтайды. Саясат Жергілікті қауіпсіздік саясаты қосымша құралы арқылы конфигурацияланады.

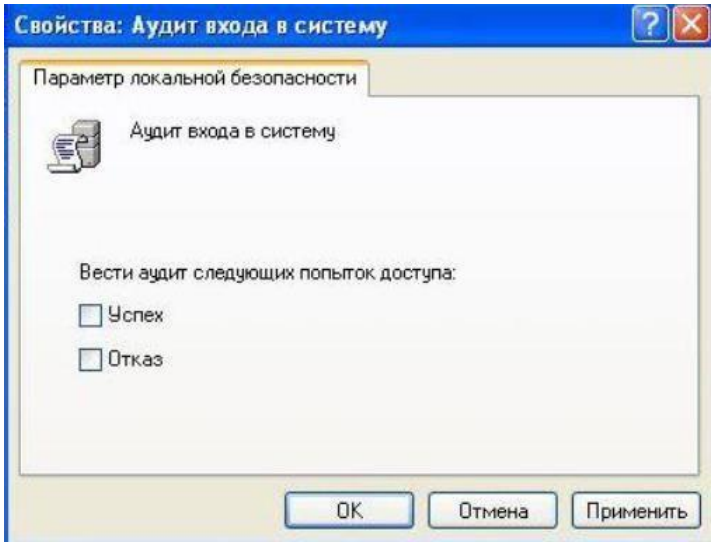
Операциялық жүйеге «Әкімші» тіркелгісі арқылы кіріңіз. Жергілікті қауіпсіздік саясаты қосымшасын ашыңыз (Бастау - Басқару тақтасы - Әкімшілік құралдар). «Жергілікті саясат - аудит саясаты» бөлімін таңдаңыз (1-сурет).



Сурет. 1 - Windows XP аудит саясаты

Аудит саясаты қауіпсіздік оқиғаларының әртүрлі санаттарына сәйкес келетін опциялар жинағын қамтамасыз етеді. Параметрлердің әрқайсысының «Сипаттары» бөлімінде сәйкес санатқа қатысты оқиғаларды жазуды қосуға болады. «Аудитке кіру» аудит саясаты параметрін ашыңыз (2-сурет). Аудит келесі оқиғалар түрлері арқылы іске қосылады:

- «Сәттілік» - қолданушыға іске асыруға рұқсат етілген оқиғалар жазылады;
- «Қабылдамау» - қолданушыға жүзеге асыруға тыйым салынған оқиғалар жазылады.



Сурет. 2 - «Аудитке кіру» параметрінің параметрлері

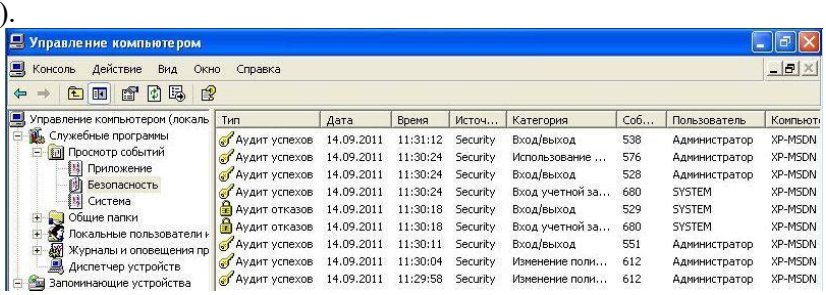
2. Пайдаланушының кіру/шығуын тексеру

Кіруді тексеру опциясы әрбір пайдаланушының осы компьютердегі жүйеге кіру немесе жүйеден шығу әрекетін жазуға мүмкіндік береді. Аудитке кіру опциясы үшін екі оқиға түрін де (сәттілік және сәтсіздік) қосыңыз.

Аудитке кіру оқиғалары опциясы үшін екі оқиға түрін де (сәттілік және сәтсіздік) қосыңыз. «Жүйеге кіру оқиғаларын тексеру» параметрі осы компьютердің тіркелгі деректерінің (соның ішінде жұмыс станциясында доменді енгізу кезіндегі домен контроллері) әрбір тексеруін жазуға мүмкіндік береді.

Ағымдағы пайдаланушының сеансын аяқтаңыз. Қабылдамау түріндегі оқиғаны жасау үшін амалдық жүйеге кіру кезінде жарамсыз құпия сөзді енгізіңіз.

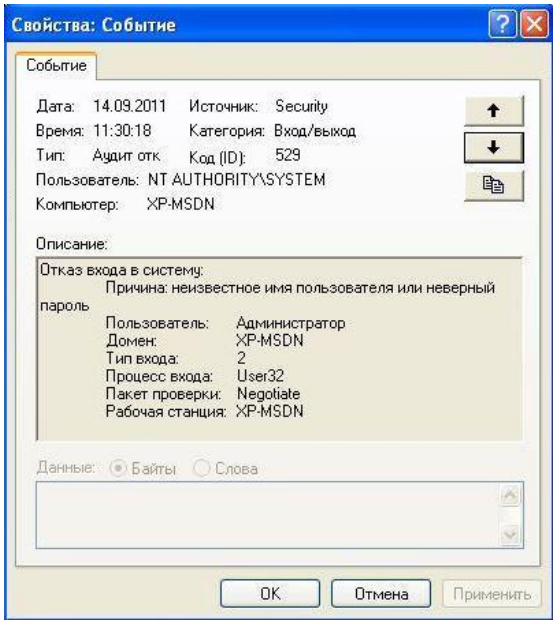
«Әкімші» тіркелгісі арқылы кіріңіз. Оқиғаларды қарау құралында қауіпсіздік журналын ашыңыз (3-сурет).



Сурет. 3 - «Қауіпсіздік» журналы

Қауіпсіздік журналының жазбалары оқиға туралы келесі ақпаратты қамтиды: оқиғаның уақыты мен күні; оқиғаны жасаған пайдаланушы тіркелгісінің атауы; оқиға орын алған компьютердің атауы; оқиғаның санаты мен түрі; оқиға коды; оқиға санатына байланысты қосымша ақпарат.

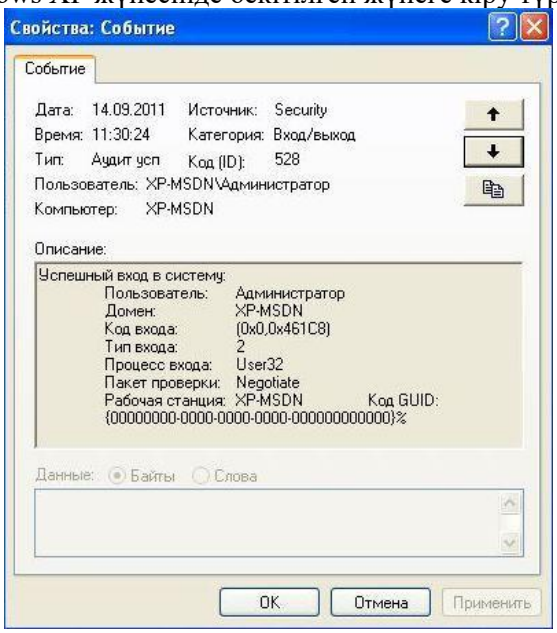
Қауіпсіздік журналында ақаулық аудиті түрінің Енгізу/Шығу санатының жазбасын ашыңыз. Бұл жазба қате құпия сөзді енгізу кезінде жасалған оқиғаны сипаттайды (Сурет 4). Пайдаланушы әлі аутентификацияланбағандықтан, оқиға «Жүйе» пайдаланушысының атынан жасалған. Оқиға жазбасы сәтсіз кіру әрекеті жасалған кезде пайдаланылған пайдаланушы атын және кіру түрін көрсетеді. Бұл оқиғаның оқиға коды 529.



Сурет. 4 - Жүйеге кіру сәтсіздігі туралы жазбаны тексеру

528 коды бар Sccess Audit түрінің Entry/Exit санатының жазбасын ашыңыз. Бұл жазба операциялық жүйеге сәтті кіру кезінде жасалған оқиғаны сипаттайды (Сурет 5).

Екі жазбада да (сәттілік және сәтсіздік аудиттері) кіру түрі 2. Бұл түр интерактивті кіруді көрсетеді. Windows XP жүйесінде бекітілген жүйеге кіру түрлері бірінші кестеде көрсетілген.



Сурет 5 - Операциялық жүйеге сәтті кіруді тексеру жазбасы

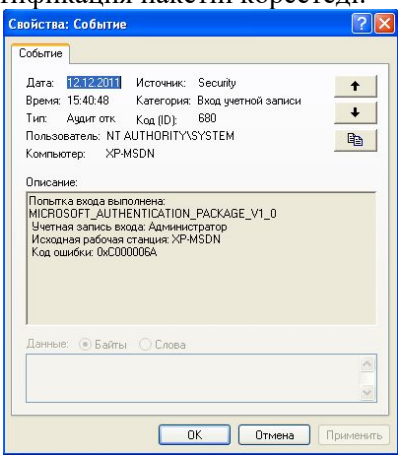
Кесте 1. Жүйеге кіру түрлерінің сипаттамасы

Жүйеге кіру түрі	Енгізу түрінің атауы	Сипаттама
2	Интерактивті	Жергілікті пайдаланушының компьютерге кіруі.
3	Желі	Пайдаланушы осы компьютерге арқылы кірді тор.
4	Пакетті	Пакеттік кіру түрі пакетпен пайдаланылады серверлер.
5	Служба	**Қызметті Қызметті басқару менеджері іске қосады.**

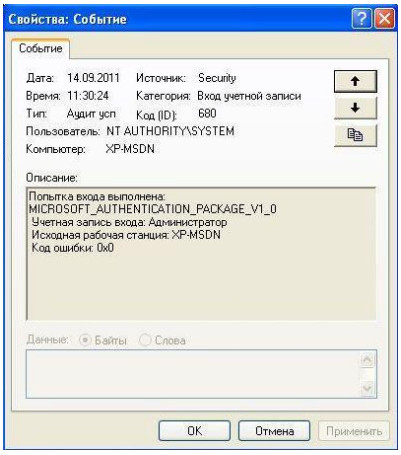
7	Разблокирование	Бұл жұмыс станциясының құлпы ашылған.
8	NetworkCleartext	Пайдаланушы осы компьютерге арқылы кірді тор. Пайдаланушы құпия сөзі өңделмеген түрде жіберілді
9	NewCredentials	Келуші өзінің ағымдағы таңбалауышын клондады және шығыс қосылымдар үшін жаңа тіркелгілерді көрсетті.
10	RemoteInteractive	Пайдаланушы Terminal Services немесе арқылы қашықтан осы компьютерге кірді қашықтағы жұмыс үстелі.
11	CachedInteractive	Пайдаланушы осы компьютерге желі тіркелгі деректерімен кірді. компьютерде жергілікті сақталған тіркелгі деректері.

551 идентификаторы бар Success Audit түріндегі Кіру/Шығу санатының жазбасын ашыңыз. Бұл жазбада пайдаланушының операциялық жүйеден сәтті шығуына қатысты ақпарат бар.

«Тіркелгіге кіру» санатының жазбаларын ашыңыз (Сурет 6, 7). Оқиғалардың екі түрінің де («Сәтті» және «Сәтсіздік») бір оқиға коды бар - 680. Сонымен қатар, жазба аутентификация механизмін - Microsoft аутентификация пакетін көрсетеді.



Сурет. 6 - Entry Failure Audit Record
есептік жазба



Сурет. 7 - табысты аудит жазбасы
тіркелгіге кіру

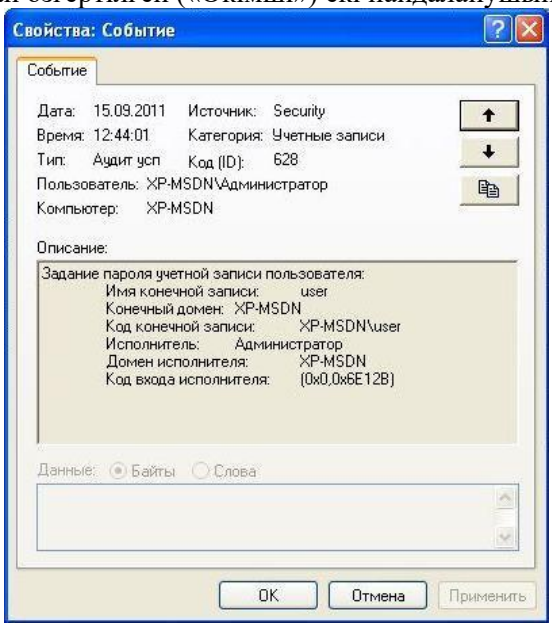
3. Әкімшілікпен байланысты оқиғаларды тексеру

"Тіркелгіні басқаруды тексеру" параметрі пайдаланушы тіркелгілері мен пайдаланушы топтарын басқаруға қатысты оқиғаларды жазуға мүмкіндік береді. «Тіркелгіні басқару аудиті» үшін «Сәтті» оқиға түрін қосыңыз.

"пайдаланушы" пайдаланушысының құпия сөзін өзгертіңіз, "user1" жаңа пайдаланушысын жасаңыз. Тіркелгіні басқару аудиті санатындағы жазбалар тіркелгі атауын да қамтиды

өзгертілген жазба және параметрлерді өзгерткен пайдаланушы тіркелгісінің атауы.

Оқиға идентификаторы 628 бар «Қауіпсіздік» журналында «Тіркелгілер» санатының жазбасын ашыңыз (егер жазба болмаса, журналды жаңартыңыз). Бұл жазба тіркелгі құпия сөзін өзгерту туралы ақпаратты қамтиды (Сурет 8). Тексеру жазбасында құпия сөзі өзгертілген («пайдаланушы») және оның атынан өзгертілген («Әкімші») екі пайдаланушының тіркелгі атаулары көрсетіледі.



Сурет. 8 - Тіркелгі құпия сөзін сәтті өзгертудің аудит жазбасы

626 оқиға идентификаторы бар «Тіркелгілер» санатындағы жазбаны ашыңыз. Бұл жазбада пайдаланушы тіркелгісін қосу (жаңа жасау) туралы ақпарат бар (9-сурет).

Жаңа пайдаланушы жасалғанда, ол автоматты түрде топқа қосылады. 636 оқиға идентификаторы бар «Тіркелгілер» санатындағы жазбаны ашыңыз. Бұл жазбада бар топқа пайдаланушы тіркелгісін қосу туралы ақпарат бар (Сурет 10). Жазбада қосқан пайдаланушының тіркелгі атауы, қосылатын пайдаланушының тіркелгі атауы және пайдаланушы қосылған топтың аты бар.

«Аудит саясатындағы өзгерістер» опциясы аудит саясатындағы өзгерістерге, пайдаланушыларға құқықтарды беруге және т.б. байланысты оқиғаларды жазуға мүмкіндік береді. «Аудит саясатын өзгерту» үшін «Сәтті» оқиға түрін қосыңыз.

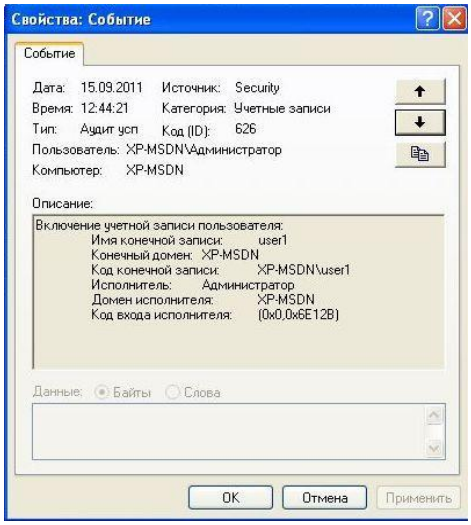
«Жергілікті саясаттар - пайдаланушы құқықтарын тағайындау» бөлімін ашыңыз

«Жергілікті қауіпсіздік саясаты». Пайдаланушыға «пайдаланушыға» құқық беріңіз

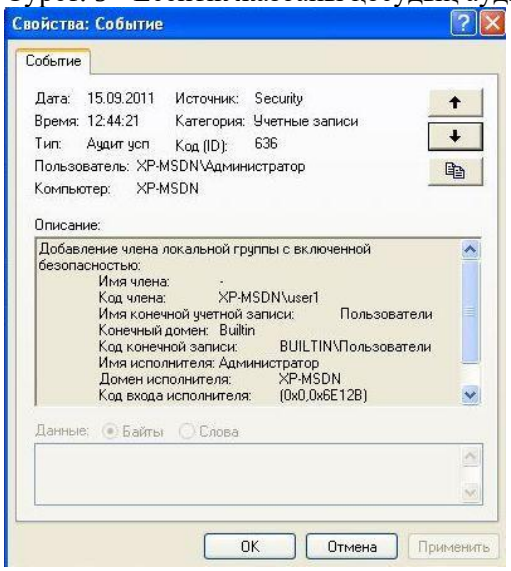
«Файлдар мен каталогтарды мұрағаттау», «Қонақ» тіркелгісінен «Жергілікті түрде кіру» опциясын алып тастаңыз.

Аудит саясатын өзгерту санатындағы жазбалар саясатты өзгерткен тіркелгінің атауын, өзгертілетін артықшылықтың немесе параметрдің атауын қамтиды. Егер пайдаланушы тіркелгісінің артықшылығы өзгерсе, осы тіркелгінің атауы көрсетіледі.

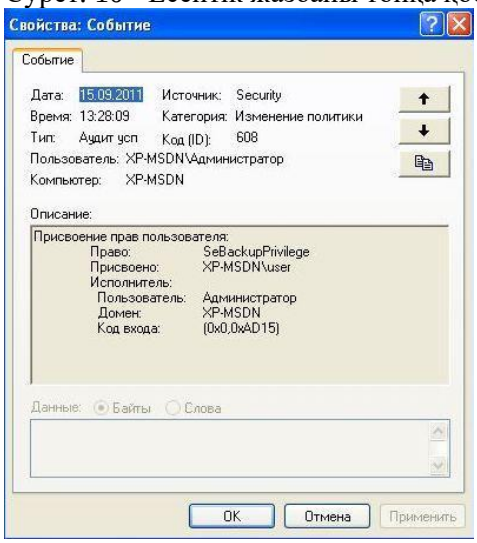
608 коды бар «Саясатты өзгерту» санатындағы жазбаны ашыңыз (11-сурет). Бұл жазба пайдаланушыға ақпараттың сақтық көшірмесін жасау құқығын беру туралы ақпаратты қамтиды (SeBackupPrivelege).



Сурет. 9 - Есептік жазбаны қосудың аудит жазбасы



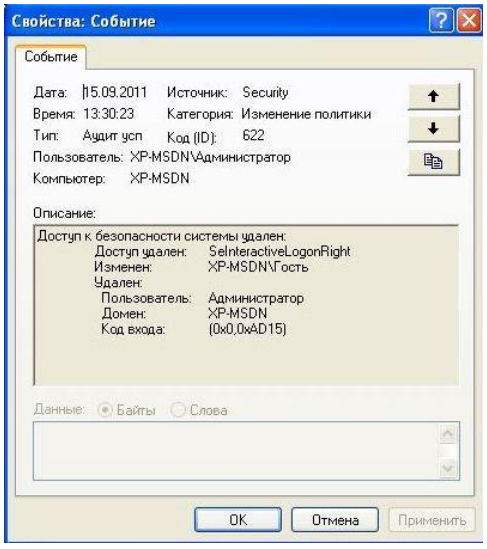
Сурет. 10 - Есептік жазбаны топқа қосу туралы тексеру жазбасы



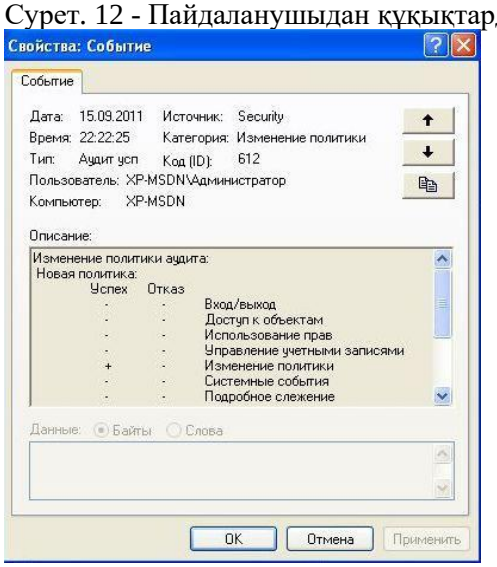
Сурет. 11 - Пайдаланушыға құқықтарды беру аудитінің жазбасы

622 коды бар «Саясатты өзгерту» санатындағы жазбаны ашыңыз (12-сурет). Бұл жазба пайдаланушының жергілікті кіру құқығын (SeInteractiveLogonRight) жою туралы ақпаратты қамтиды.

612 коды бар «Саясатты өзгерту» санатындағы жазбаны ашыңыз (13-сурет). Бұл жазба аудит саясатын өзгерту туралы ақпаратты қамтиды. «Саясатты өзгерту» санатына «Табыс» аудитін қосу түзетілді.



Сурет. 12 - Пайдаланушыдан құқықтарды жою туралы аудитті жазу

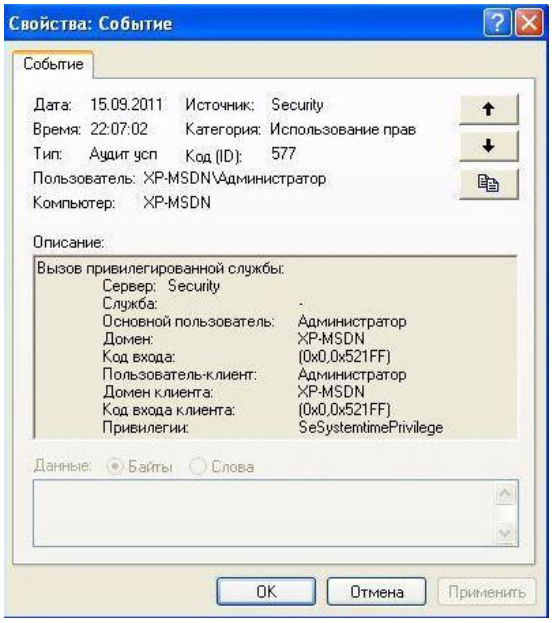


Сурет. 13 - Қауіпсіздік саясатының өзгеруінің аудит жазбасы

«Артықшылықтарды пайдалануды тексеру» параметрі пайдаланушының өзіне берілген артықшылықтарды пайдалануына байланысты оқиғаларды жазуға мүмкіндік береді. «Аудит артықшылығын пайдалану» үшін «Сәтті» оқиға түрін қосыңыз.

Жүйе уақытын өзгертіңіз. Пайдаланушы сеансын аяқтаңыз. «Әкімші» тіркелгісі арқылы кіріңіз.

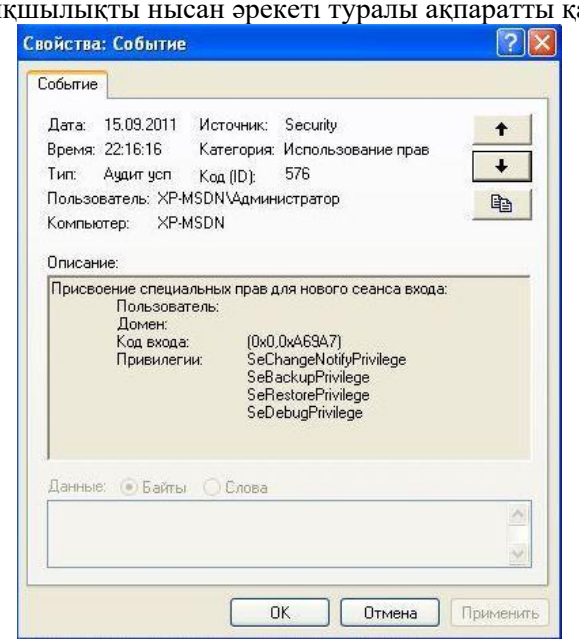
577 коды бар «Құқықтарды пайдалану» санатының жазбасын ашыңыз (14-сурет). Бұл жазба артықшылықты қолданған пайдаланушыны көрсететін жүйе уақытын (SeSystemtimePrivelege) өзгерту үшін артықшылықты пайдалану туралы ақпаратты қамтиды.



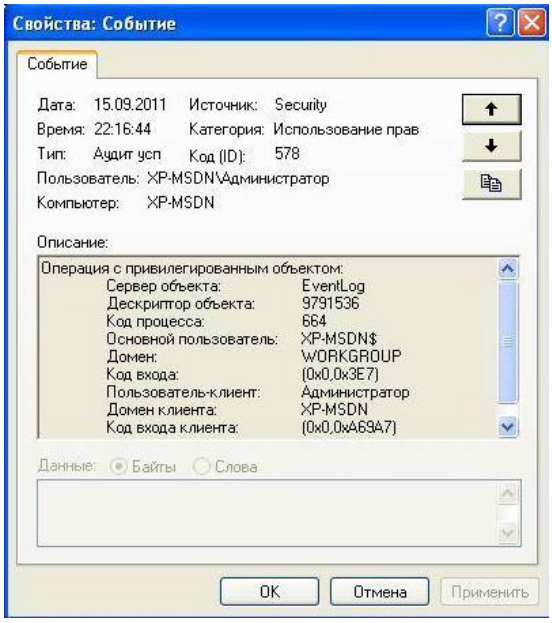
Сурет. 14-сурет - Жүйе уақытын өзгерту артықшылығын қолдану туралы аудит жазбасы 576 коды бар «Құқықтарды пайдалану» санатының жазбасын ашыңыз (15-сурет). Бұл

жазба операциялық жүйеге кіру кезінде пайдаланушыға артықшылықтар жинағын беру туралы ақпаратты қамтиды.

578 коды бар «Құқықтарды пайдалану» санатының жазбасын ашыңыз (16-сурет). Бұл жазба артықшылықты нысан әрекеті туралы ақпаратты қамтиды - аудит журналын ашу (EventLog).



Сурет. 15 - Жүйеге кіру кезінде пайдаланушыға артықшылықтарды тағайындаудың аудит жазбасы



Сурет. 16 - Аудит журналымен жұмыс істеу туралы аудитті тіркеу

4. Операциялық жүйенің жұмысына байланысты оқиғаларды тексеру

«Жүйенің оқиғаларын тексеру» параметрі келесі жүйелік оқиғалармен байланысты оқиғаларды жазуға мүмкіндік береді: жүйе уақытының өзгеруі; қауіпсіздік жүйесінің элементтерін іске қосу және өшіру және т.б. үшін "Сәтті" оқиға түрін қосыңыз

«Аудит жүйесінің оқиғалары».

Тексеру журналын өшіріңіз (мысалы, журналдың контекстік мәзірі арқылы).

Операциялық жүйені қайта жүктеңіз.

517 коды бар «Жүйелік оқиға» санатындағы жазбаны ашыңыз (17-сурет). Бұл жазбада аудит журналының қашан тазартылғаны және журналды тазалаған пайдаланушы тіркелгісінің аты туралы ақпарат бар.

520 коды бар «Жүйелік оқиға» санатының жазбасын ашыңыз (18-сурет). Бұл жазба жүйе уақытын өзгерту туралы ақпаратты қамтиды. Бұл оқиға сервермен уақытты синхрондау кезінде «Жүйе» тіркелгісінің атынан да, пайдаланушы атынан да жасалуы мүмкін. Жазба алдыңғы және жаңа уақытты көрсетеді.

«Аудиттік үдерісті қадағалау» параметрі процестердің жұмысына байланысты оқиғаларды тіркеуді (жасау, тоқтату, қайталау және т.б.) қамтиды. «Процессті бақылау аудиті» үшін «Сәтті» оқиға түрін қосыңыз.

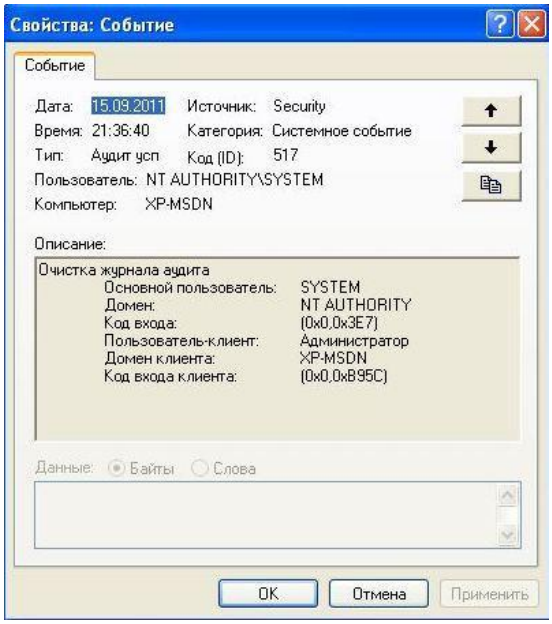
Кез келген қолданбаны іске қосыңыз және оны жабыңыз.

592 және 593 коды бар «Егжей-тегжейлі қадағалау» санатындағы жазбаларды ашыңыз (19, 20-сурет). Бұл жазбалар жаңа процесті құру және оны тоқтату туралы ақпаратты қамтиды. Оқиға туралы ақпарат процесті бастаған орындалатын файлдың толық атауын қамтиды.

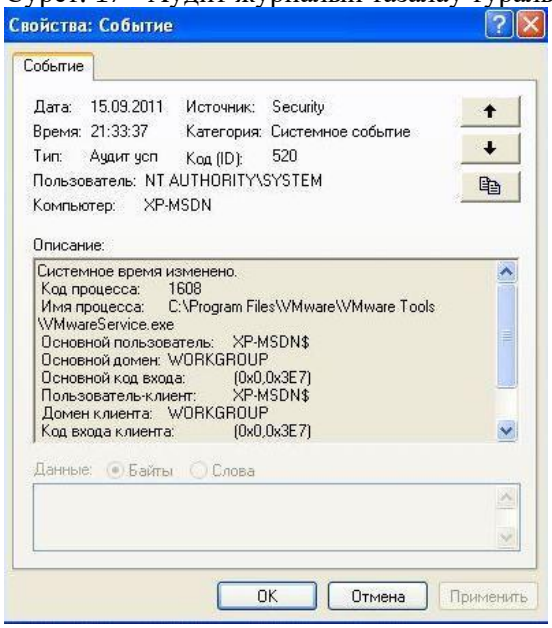
5. Пайдаланушының ресурстарға қол жеткізуін тексеру

«Объектілерге қол жеткізуді тексеру» параметрі файлдарға, каталогтарға, тізілім кілттеріне, принтерлерге және т.б. кіруге қатысты оқиғаларды жазуды қамтиды. Қол жеткізудің әртүрлі түрлерін тексеруге болады: оқу, өзгерту, жою, басып шығару және т.б.

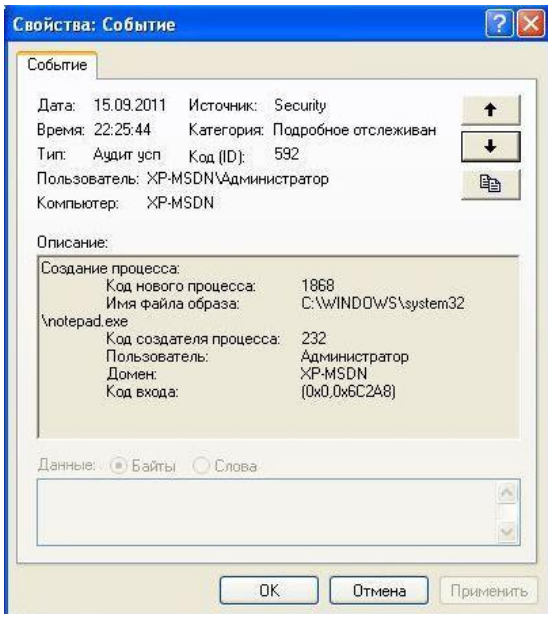
Аудит нысанына қатынасу опциясы үшін екі оқиға түрін де (сәттілік және сәтсіздік) қосыңыз.



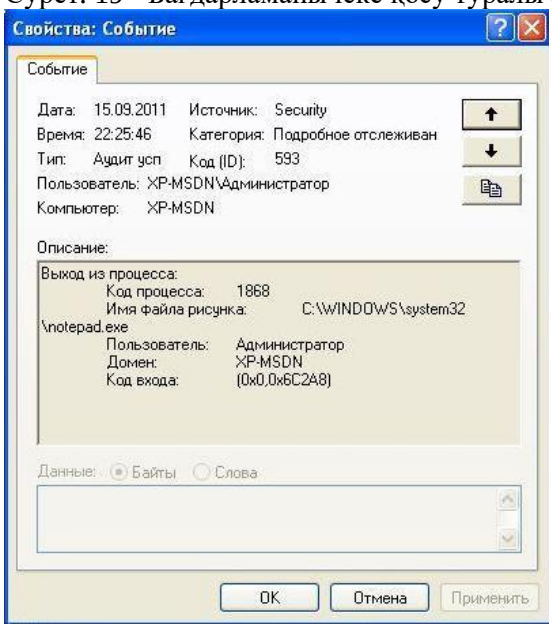
Сурет. 17 - Аудит журналын тазалау туралы аудит жазбасы



Сурет. 18 - Жүйе уақытының өзгеруінің аудит жазбасы



Сурет. 19 - Бағдарламаны іске қосу туралы аудит жазбасы (процесті құру)



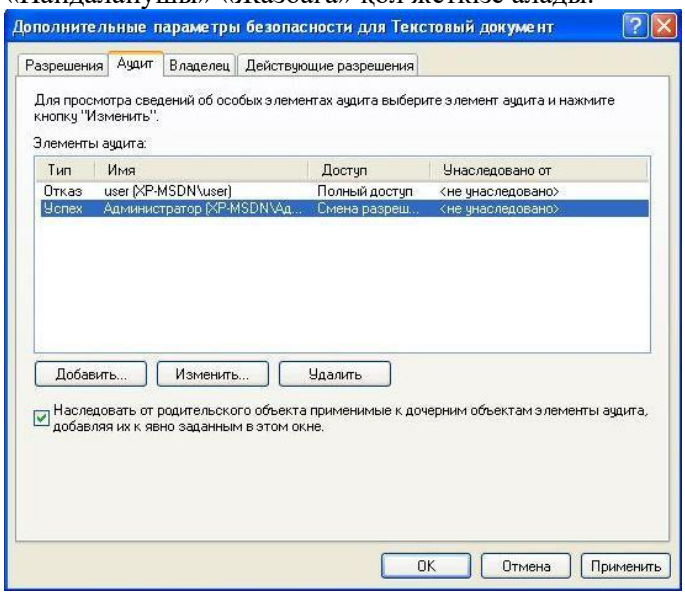
Сурет. 20 - Өтінімнің тоқтатылуының аудит жазбасы (процестің шығуы)

Ресурстарға қол жеткізуді тексеру NTFS файлдық жүйесі бар логикалық дискілерде ғана мүмкін болады. Тек оқиғаларды түсіру қажеттілігі нақты көрсетілген нысандар ғана аудитке жатады. Осылайша, қол жеткізу аудитін қосу екі кезеңде орын алады: аудит саясатындағы «Объектілерге қол жеткізуді тексеруді» қосу және әрбір басқарылатын нысан үшін аудитті қосу.

Мәтіндік файл жасаңыз. Құрылған файлдың «Сипаттар» («Сипаттар - Қауіпсіздік - Кеңейтілген - Аудит») «Аудит» қойындысына өтіңіз. Пайдаланушы үшін «Рұқсаттарды өзгерту» қатынасу түріндегі «Сәтті» оқиға түрін қосыңыз

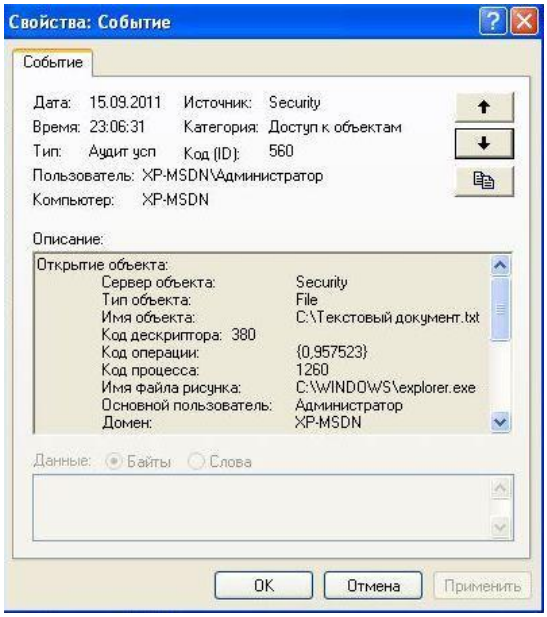
«Әкімші» және «Қабылдамау» оқиға түрі «пайдаланушы» пайдаланушыға кірудің барлық түрлеріне арналған (Сурет 21). Жасалған файлдың сипаттарының «Қауіпсіздік» қойындысында пайдаланушыға тыйым салыңыз

«Пайдаланушы» «Жазбаға» қол жеткізе алады.

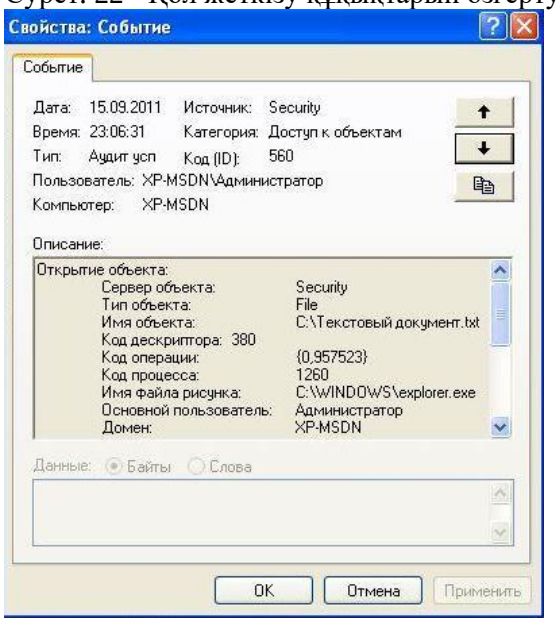


Сурет. 21 - Файлға қатынасу аудитінің опциялары

560 коды бар «Нысанға қол жеткізу» категориясының жазбасын ашыңыз (22, 23-сурет). Бұл жазба нысанға кіру рұқсаттарын сәтті өзгерту туралы ақпаратты қамтиды (қол жеткізу түрі - WRITE_DAC). Жазба рұқсат түріне қосымша рұқсат нысаны туралы ақпаратты қамтиды: аты және түрі (Файл). Қол жеткізу субъектісі туралы келесі ақпарат көрсетіледі: қол жеткізуді орындаған тіркелгінің атауы және қол жеткізу орындалған процестің орындалатын файлының толық атауы.



Сурет. 22 - Қол жеткізу құқықтарын өзгерту үшін нысанға кіру туралы жазбаны тексеру



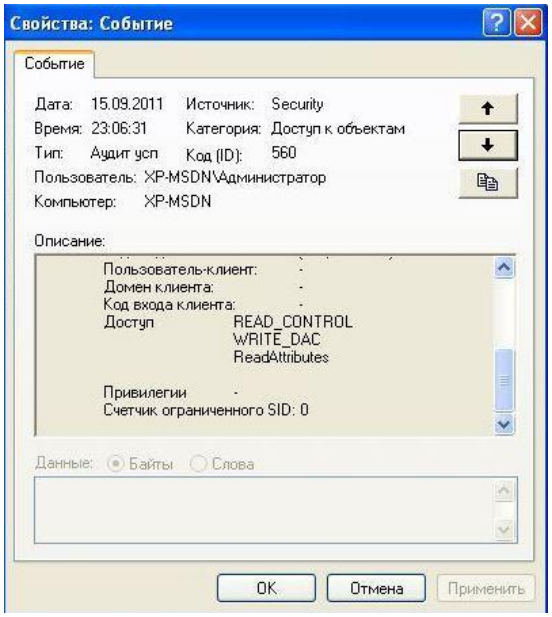
Сурет. 23 - Қол жеткізу құқықтарын өзгерту үшін нысанға қатынасу туралы аудитті жазу (соңы)

«пайдаланушы» ретінде кіріңіз. Жасалған файлды жоюға тырысыңыз,

файлдағы рұқсаттарды өзгертіп көріңіз.

«Әкімші» тіркелгісі арқылы кіріңіз. Журнал жазбаларын ашыңыз

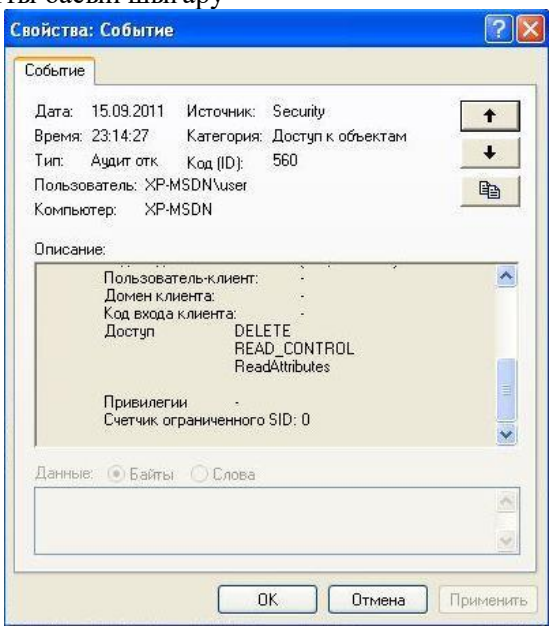
«Пайдаланушы» тіркелгісінің атынан орындалатын 560 коды бар «Объектіге қол жеткізу» санатының «Қауіпсіздігі». Жазбалардың бірінде файлды жоюдың сәтсіз (Аудит қателері) әрекеті туралы ақпарат бар (қол жеткізу түрі - DELETE, 24-сурет). Басқа жазбада файлға кіру рұқсаттарын өзгертуге сәтсіз әрекет (Аудит қателері) туралы ақпарат бар (Сурет 25).



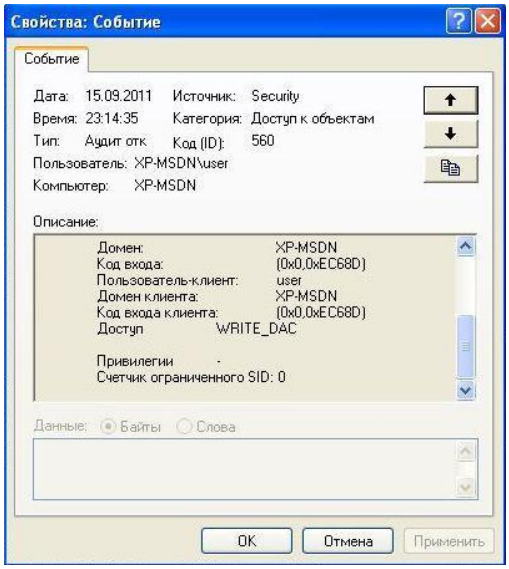
Сурет. 24 - Объектіні жою әрекетінің сәтсіздігінің аудит жазбасы doPDF принтерінің «Сипаттар» тармағын ашыңыз («Бастау - Параметрлер - Принтерлер мен факстар»).

Принтерлер үшін келесі нақты әрекеттерді тексеруге болады: басып шығару, принтерді басқару, құжатты басқару.

«Әкімші» пайдаланушысы үшін doPDF принтерінің «Құжаттарды басқару» қол жеткізу түрінің «Сәтті» аудит түрін қосыңыз («Осы принтер және құжаттар үшін» қолданбасы, 26-сурет). Мәтіндік құжатты басып шығару

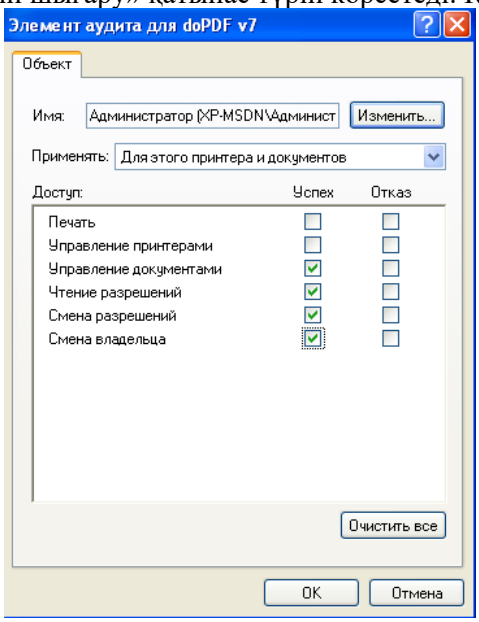


Сурет. 25 - Объектіге қол жеткізу құқығын өзгерту үшін оған қол жеткізудің сәтсіз әрекетінің аудит жазбасы

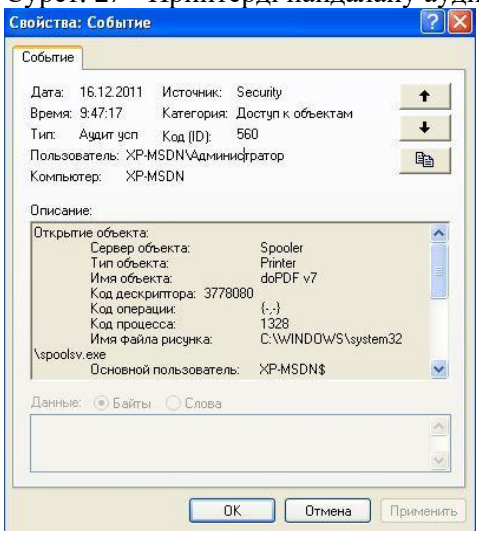


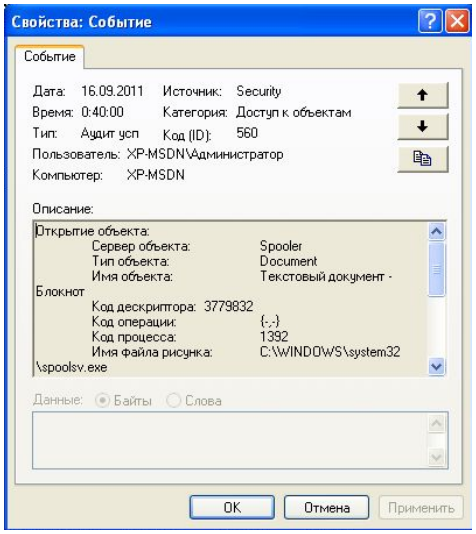
Сурет. 26 - Принтерге қол жеткізу аудитінің параметрлері

560 коды бар «Нысанға қол жеткізу» санатындағы жазбаларды қараңыз. Принтер (27-сурет) және Құжат (28-сурет) нысан түрі бар жазбалар құжатты басып шығаруға қатысты. Принтерге арналған жазба «Басып шығару» қатынас түрін көрсетеді. Құжат жазбасы басып шығарылған құжаттың атауын қамтиды.



Сурет. 27 - Принтерді пайдалану аудитінің жазбасы



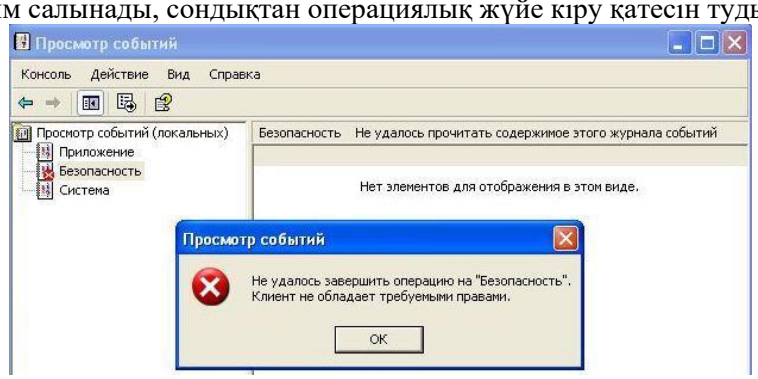


Сурет. 28 - Құжат айналымын тексеру есебі

6. Аудит ізін басқару

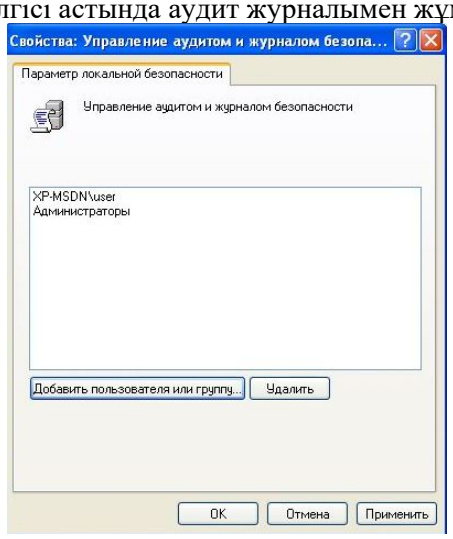
«Пайдаланушы» тіркелгісімен кіріңіз. Тексеру журналын ашуға тырысыңыз. топ

«Пайдаланушы» кіретін «Пайдаланушылар» әдепкі бойынша аудит журналымен жұмыс істеуге тыйым салынады, сондықтан операциялық жүйе кіру қатесін тудырады (Сурет 29).



Сурет. 29 - Аудит журналына кіру қатесі

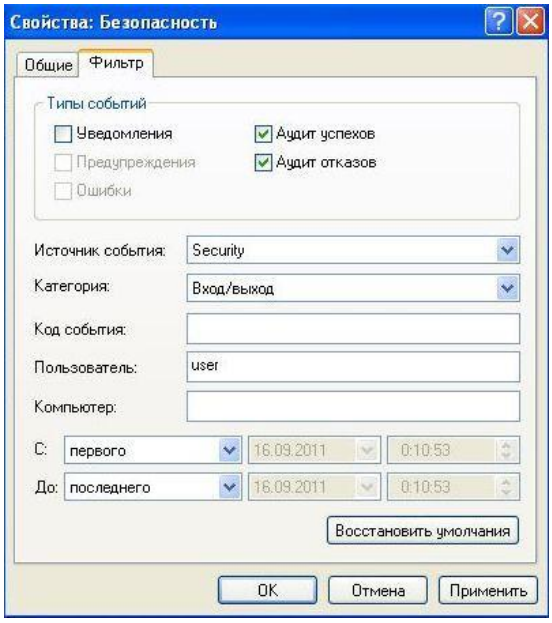
Жергілікті қауіпсіздік саясаты қосымшасын әкімші тіркелгісі ретінде іске қосыңыз. «Аудит және қауіпсіздік журналын басқару» параметріндегі тіркелгілер тізіміне «пайдаланушы» пайдаланушысын қосыңыз («Жергілікті саясаттар - Пайдаланушы құқықтарын тағайындау», 30-сурет). «Пайдаланушы» тіркелгісі астында аудит журналымен жұмыс істеу құқықтарын тексеріңіз.



Сурет. 30 - Қауіпсіздік журналына кіруді басқару опциясы

«Әкімші» тіркелгісі арқылы кіріңіз. Аудит журналы мәзірінен таңдаңыз

«Көру» - «Сүзгі». Сүзгіні суретке сәйкес реттеңіз. 31. Сүзгіні қолданғаннан кейін журналда «пайдаланушы» тіркелгісі бойынша сәтті және сәтсіз кіру әрекеттері туралы жазбалар ғана қалады.



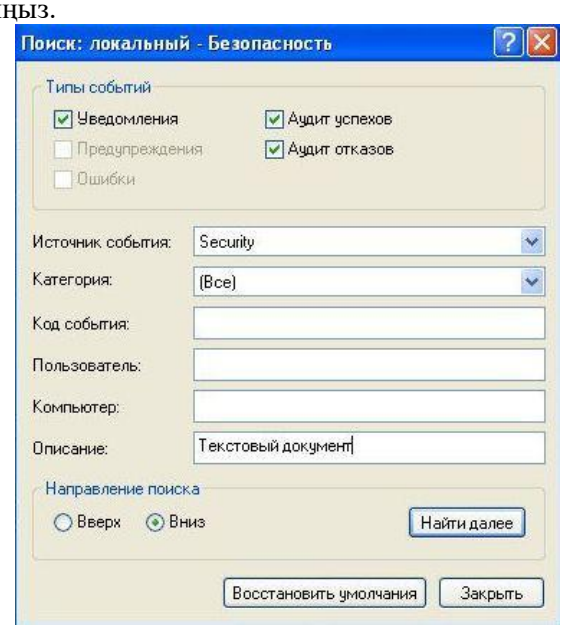
Сурет. 31 - Қауіпсіздік журналының енгізуін сүзуді конфигурациялау

Белгілі аты бар нысанды іздеген кезде іздеу функциясын қолданған дұрыс:

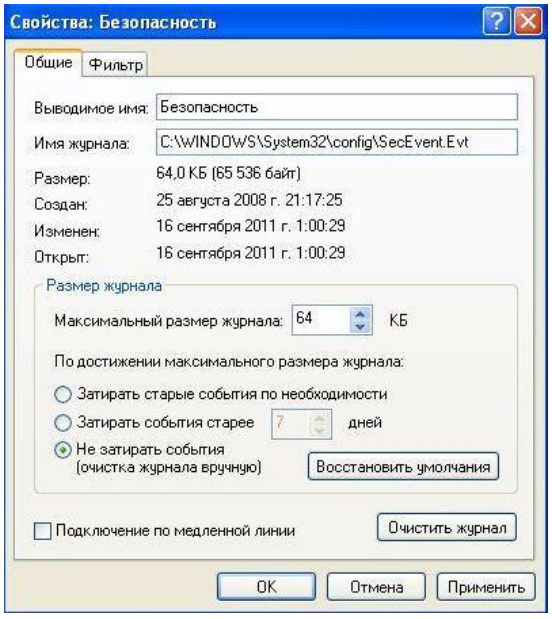
«Көру» - «Табу» (32-сурет), файлдың атын (атаудың бөлігін) енгізіңіз.

Қауіпсіздік журналының мәтінмәндік мәзірінен Сипаттар тармағын таңдаңыз. Пайда болған қойындыда журналдың ең үлкен өлшемін және ол толған болса не істеу керектігін орнатуға болады (Сурет 33).

Журнал өлшемін ең кіші мүмкін мәнге орнатыңыз - 64 КБ. Аудиттің барлық мүмкін түрлерін қосыңыз.

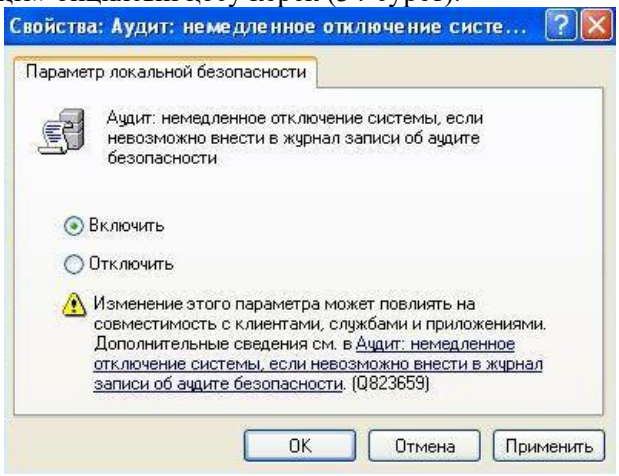


Сурет. 32 - Қауіпсіздік журналының жазбаларын іздеуді конфигурациялау



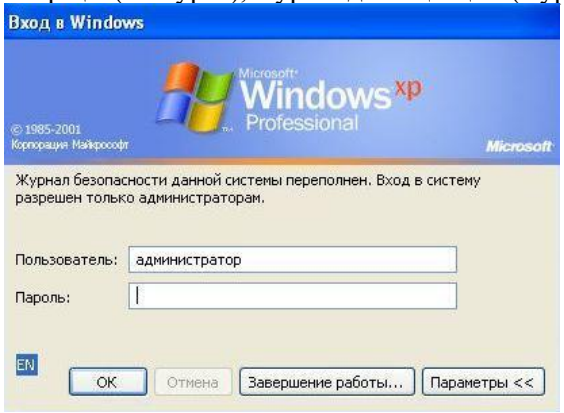
Сурет. 33 - Қауіпсіздік журналының жұмысын конфигурациялау

Журнал толтырылған кезде пайдаланушыны өшіру үшін жергілікті топ саясатының «Қауіпсіздік параметрлері» бөлімінде «Аудит: қауіпсіздік аудиті жазбаларын тіркеу мүмкін болмаса, жүйені дереу өшіріңіз» опциясын қосу керек (34-сурет).

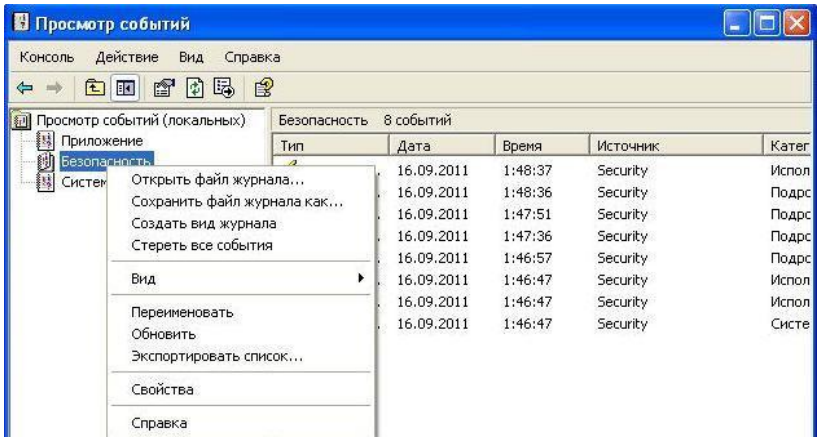


Сурет. 34 - Қауіпсіздік журналы толған кездегі әрекеттерді конфигурациялау

Операциялық жүйені қайта жүктеңіз. «Әкімші» тіркелгісі арқылы кіріңіз. Журнал толтырылғанша және жүйе қайта жүктелгенше жаңа аудит жазбаларын жасаңыз. Осыдан кейін «Әкімші» тіркелгісімен жүйеге кіріңіз (35-сурет), журналды сақтаңыз (Сурет 36) және оны тазалаңыз.



Сурет. 35 - Қауіпсіздік журналының толып кетуіне кіру терезесі



Сурет. 36 - Қауіпсіздік журналын сақтаңыз

Сақталған қауіпсіздік журналдарын қарау қауіпсіздік журналының контекстік мәзірінің «Журнал файлын ашу» функциясы арқылы жүзеге асырылады.

Тапсырма

Таңдауыңызға сәйкес қауіпсіздік журналын импорттаңыз. Варианттарды бөлу бойынша қауіпсіздік журналын талдаңыз және кінәлілерді анықтаңыз. Оқиғаларды түсіру кезінде пайдаланылатын аудит опциялары 1-кестеде келтірілген. 2. "Сақтық көшірме жасау және қалпына келтіру құқықтарын тексеру" опциясы да қосылған. Тексеру мен қауіпсіздік журналын басқару құқығы тек «Әкімші» және пайдаланушы «Анатолий» болуы мүмкін. Есептік жазбалар туралы ақпарат 3 кестеде көрсетілген.

Кесте 2. Параметры политик аудита

Название параметра	***Успех***	***Отказ***
Аудит событий входа в систему	+	+
Аудит управления учётными записями	+	+
Аудит доступа к службе каталогов	-	-
Аудит входа в систему	+	+
Аудит доступа к объектам	+	+
Аудит изменения политики	+	+
Аудит использования привилегий	-	+
Аудит отслеживания процессов	-	-
Аудит системных событий	+	+

Кесте 3. Учётные записи

Имя учетной записи	***Должность, группа***
Дмитрий	стажёр, пользователь
Геннадий	финансовый менеджер, пользователь
Василий	оператор пульта видеонаблюдения, пользователь
Администратор	технический консультант, администратор системы
Валерий	директор, оператор архива
Людмила	бухгалтер, пользователь
Татьяна	секретарь, пользователь
Артур	помощник технического консультанта, пользователь
Анатолий	администратор безопасности, администратор системы
ДАВЫДОВ	руководитель отдела разработки, пользователь

1 нұсқа

Қауіпсіздік әкімшісі Анатолий тек интерн Дмитрийге департаменттің қауіпсіздік материалдарына толық рұқсат берді. Бұл материалдар бұрын оқу, жазу, жою, сондай-ақ иесін өзгерту үшін тексерілген «Enterprise Resources\Exchange\Dmitry» желілік ресурсында орналастырылды. Құжаттарды жою кезінде Анатолий осы материалдардың басып шығарылған көшірмелерін тапты. Тағылымдамадан өтуші маңызды құжаттардың басып шығарылған көшірмелеріне өзінің қатысы жоқтығын растайды. Дмитрийдің басылған құжаттарға қатысын дәлелдеңіз немесе жоққа шығарыңыз.

2-нұсқа

Кәсіпорында «Кәсіпорын ресурстары \ Негізгі өнімнің бәсекеге қабілеттілігі» желілік ресурсы бар, онда «Бәсекелестердің өнімдері.doc» және «Негізгі өнімнің даму стратегиясы.doc» екі құжат болды. Тек келесі пайдаланушылар жазу және оқу мүмкіндігіне ие болды: «Геннадий» және «ДАВЫДОВ».

Қауіпсіздік әкімшісі Анатолий осы ресурс үшін жоюды, оқуды, жазуды, рұқсатты өзгертуді және меншік құқығын өзгертуді сәтті және сәтсіз тексеруді бұрын конфигурациялаған. Көп ұзамай қаржы менеджері мен даму бөлімінің басшысы бұл құжаттардың жоғалып кеткенін хабарлады. Осы құжаттарды алып тастауға кімнің қатысы барын анықтаңыз?

3-нұсқа

Жүйе әкімшісі пайдаланушы құпия сөздерін өзгертуді қоса алғанда, оның тіркелгісі бойынша біреу орындаған жүйелік әрекеттерді бірнеше рет хабарлады. Қауіпсіздік әкімшісі тіркелгілер мен олардың құпия сөздерін жасырын түрде сақтайтын тізілім бөлімшесіне толық аудит орнату қажет деп санады. Тіркелгі дерекқорын сақтайтын тізілім бөлімшесі келесі жолға ие:

"HKEY_LOCAL_MACHINE\SAM\SAM". Тіркелгі дерекқорына кім және қандай бағдарлама кіретінін біліңіз.

4-нұсқа

Ұйымнан өз өтініші бойынша жүйелік әкімші бір жұмыс аптасы да жұмыс істемей жұмыстан шықты. Бірнеше күннен кейін бейнебақылау пультінің операторы компьютердің оғаш әрекеті туралы хабарлады: «Компьютер өздігінен құлыпталып, MS_Support_tech567 пайдаланушысы құлыптау терезесін көрсетті». Бұғаттау себебін біліңіз.

5-нұсқа

Кәсіпорынның желілік ресурстарында қызметкерлер арасында маңызды электрондық құжаттарды алмасу кезінде қосымша қорғау шарасы парольді орнату болып табылады. Хатшы қауіпсіздік әкімшісіне мұндай қорғаныс шараларының тиімсіздігі туралы ескертті, мысал ретінде өңделген құжатты келтірді «Қызметкерлердің сәуір айындағы қызметі. doc» сақталған түпнұсқамен салыстырғанда. Қауіпсіздік әкімшісі "C:\Enterprise Resources\Exchange" желілік ресурсында онда жасалған файл нысандары үшін аудит параметрлерінің мұралануын пайдалана отырып, оқу аудитін конфигурациялады. Осы ресурстың файлдық объектілеріне олар үшін құпия сөзді табу фактісіне аудит жүргізіңіз.

6-нұсқа

Кәсіпорынның тек пошта серверлерімен жұмыс істеу үшін конфигурацияланған Интернетке кіру мүмкіндігі бар. Интернетке қолжетімділікті қамтамасыз ету үшін кіріс шоттары пошта хаттамалары арқылы алынған трафик көлеміне сәйкес келмейді. Директор қауіпсіздік әкімшісінен мұндай шығындардың себебін анықтауды сұрады. Интернеттен деректердің үлкен көлемін ала алатын пайдаланушылар іске қосқан бағдарламалардың аудитін жүргізіңіз.

7-нұсқа

Қауіпсіздік әкімшісі ұйымның компьютерлерінде қолданылатын лицензияланған бағдарламалық құралға жауапты. Сондықтан ол 25 таңбалы Windows өнім кілті сияқты жеке лицензияланған бағдарламалық құрал ақпаратын ұрлауға әкелетін ақпаратқа қол жеткізуді қадағалауы керек. Бұл ақпараттың көпшілігі оқу аудитіне жататын тізілім бөлімдерінде сақталады. Лицензияланған бағдарламалар тізілімінің филиалдарының мәндерін, сондай-ақ пайдаланылған бағдарламаларды оқығаныңыз үшін қауіпсіздік журналын тексеріңіз.

8-нұсқа

Ұйымның директоры файл үшін кірістірілген сақтық көшірме құралдарын пайдаланады

Ол мұрағатын «C:\ARCHIVE\backup» папкасына сақтайтын, тек өзі ғана қол жеткізе алатын «Заказ базасы.doc». Ұйымның ішкі қауіпсіздік тобы расталған жіберушілер тізімінде жоқ жалған жіберуші мекенжайы бар сүзгіден өткен электрондық пошта туралы хабарлады. Хат мәтінінде ақпаратты сату туралы ұсыныс және директор мұрағатындағы файлды қамтитын электронды құжаттар тізімі бар. Қауіпсіздік әкімшісіне қол жеткізу шектелген файлдарды алу жолын анықтау мәселесін қамтитын ақпараттың ағып кету мәселелерін шешу тапсырылды. Қол жеткізуге тыйым салынған файлды кім және қалай алғанын біліңіз.

9-нұсқа

Қауіпсіздік әкімшісі ұйымның сенімсіз қызметкерлерін тексеру қажет деп санады. Ол үшін құжатқа қол жеткізуді ашты

оқу және жазу аудитін тағайындау арқылы «қызметкерлердің жалақысы 30.04.09.doc. Осы файлды өңдеген сенімсіз пайдаланушыларды анықтаңыз.

10-нұсқа

Әкімші ұйымның компьютерлерінде үнемі қайта пайда болатын, соның ішінде орнату үшін жергілікті әкімші құқықтарын талап ететін қажетсіз бағдарламалық қамтамасыз етудің (компьютерлік ойындар) болуына шағымданды. Қай пайдаланушылардың жергілікті әкімші құпия сөзі бар екенін анықтау үшін аудит жүргізіңіз.

Тест сұрақтары

1. Жүйеге кіру/шығу аудиті кезінде қандай деректер алынады?
2. Кіру аудитінің кіру оқиғаларын тексеруден айырмашылығы неде?
3. Есептік жазбаны басқару аудиті кезінде қандай деректер алынады?
4. Саясаттың өзгеруі тексерілгенде қандай деректер алынады?
5. Құқықтарды пайдалану аудиті кезінде қандай деректер жазылады?
6. Жүйе оқиғаларын тексеру кезінде қандай деректер алынады?
7. Процесті бақылау аудитінде қандай деректер алынады?
8. Объектілерге қол жеткізуді тексеру кезінде объектілердің қандай түрлерін жасауға болады? Қандай деректер түсіріледі?
9. Объектіге қол жеткізу аудиті қалай конфигурацияланады?
10. Аудитке қатысты қауіпсіздік саясатының параметрлері қандай?

Тапсырма

Зертханалық есеп нұсқаулықта сипатталған стандартқа сәйкес орындалады

ОЖҚ. Зертханалық жұмыс № 15. ОПЕРАЦИЯЛЫҚ ЖҮЙЕНІҢ ҚАУІПСІЗДІК ПАРАМЕТРЛЕРІН ТАЛДАУ ЖӘНЕ КОНФИГУРАЦИЯЛАУ

Зертханалық жұмыстың мақсаты: қауіпсіздік ішкі жүйесінің ағымдағы күйін бағалау және қауіпсіздік параметрлерінің тұтастығын бақылау үшін Windows амалдық жүйесіне енгізілген мүмкіндіктермен танысу.

Зертханалық жұмыстың міндеттері:

1. Қауіпсіздік үлгісінің құрылымы
2. Қауіпсіздік үлгілерін басқару
3. Операциялық жүйенің қауіпсіздік параметрлерін талдау
4. Операциялық жүйенің қауіпсіздік параметрлерін орнату
5. Тапсырма
6. Бақылау сұрақтары

Зертханалық жұмыстың мазмұны:

Ағымдағы жағдайды бағалау қауіпсіздік параметрлерінің ағымдағы мәндерін эталондық мәндермен салыстыру негізінде жүзеге асырылады. Эталонды қолдану операциялық жүйенің қауіпсіздігін орнатуды автоматтандыруға және белгіленген қауіпсіздік деңгейін одан әрі бақылауға мүмкіндік береді.

Windows XP операциялық жүйесінде ағымдағы және анықтамалық қауіпсіздік параметрлерімен жұмыс істеу үшін қауіпсіздік үлгілері және қауіпсіздікті талдау және теңшеу жабдықтары бар.

Амалдық жүйеге әкімші тіркелгісімен кіріңіз. Microsoft Management Console бағдарламасын ашыңыз ("Бастау - Іске қосу "және" mmc "пәрменін енгізіңіз) және" қауіпсіздікті талдау және конфигурациялау "және"қауіпсіздік үлгілері" құралдарын қосыңыз.

1. Қауіпсіздік үлгісінің құрылымы

Қауіпсіздік үлгісі-ақпараттық қауіпсіздікке әсер ететін операциялық жүйенің анықтамалық параметрлерінің жиынтығы. Windows XP жүйесінде кірістірілген қауіпсіздік үлгілерінің жиынтығы бар. Әдепкі бойынша кірістірілген қауіпсіздік үлгілері каталогта орналасқан C:\Windows\security\templates\. Үлгіге кіретін параметрлерді қарау және өңдеу қауіпсіздік шаблондары арқылы жүзеге асырылады (сурет. 1).

Төменде кірістірілген қауіпсіздік үлгілерінің тізімі және олардың қысқаша сипаттамасы берілген.

а) әдепкі қауіпсіздік (Setup security.inf) - операциялық жүйені орнату кезінде әдепкі бойынша қолданылатын қауіпсіздік параметрлерін, соның ішінде жүйелік дискінің түбірлік каталог файлдарының рұқсаттарын қамтиды. Бұл үлгіні апатты қалпына келтіру мақсатында толығымен немесе ішінара пайдалануға болады.

б) үйлесімді (Compatws.inf) - жұмыс станциялары мен серверлер үшін әдепкі рұқсаттарды қамтиды (Домен контроллері емес). Жергілікті топтардың құқықтарының иерархиясы ескеріледі:" әкімшілер"," тәжірибелі пайдаланушылар "және"пайдаланушылар".

в) қорғау (Securews.inf және Securedc.inf) - жұмыс станцияларын теңшеуге арналған шаблондар (ws

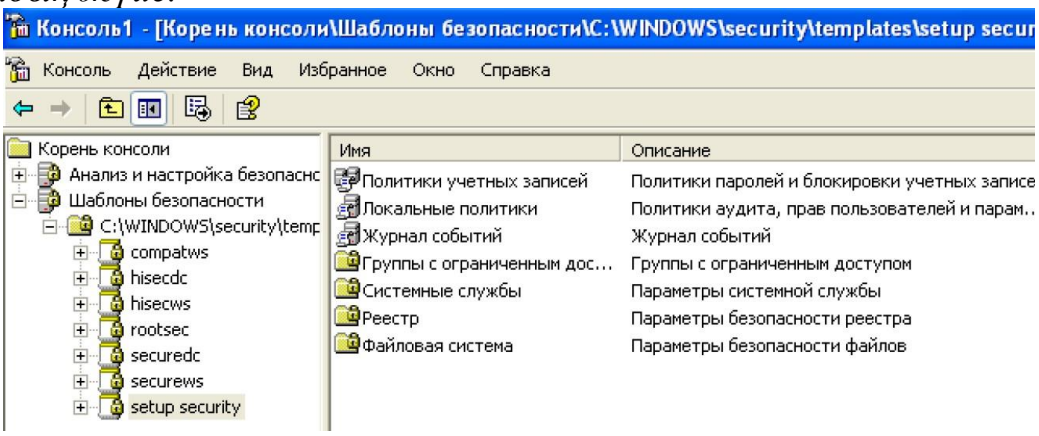
- workstations) және домен контроллері (dc - domain controllers). Олар жоғары қауіпсіздік параметрлерін анықтайды: күшті парольдер, құлыптау және аудит параметрлері анықталады; NTLM протоколымен жұмыс істеу ережелері; анонимді пайдаланушылар үшін қосымша шектеулер анықталады.

г) жоғары қорғаныс (Hisecws.inf және Hisecdc.inf) - жұмыс станциялары мен Домен контроллерлеріне арналған қосымша қорғаныс үлгілері *SMB клиенттері мен серверлері арасында Қауіпсіз арналар арқылы берілетін деректердің түпнұсқалығын тексеру үшін қажетті кодтау және қолтаңба деңгейлеріне шектеулер.*

д) жүйелік түбірлік каталогтың қауіпсіздігі (Rootsec.inf) - жүйелік дискінің түбірлік каталогы үшін қолданылатын әдепкі рұқсаттарды қамтиды.

Әрбір үлгі келесі бөлімдерден тұрады (сурет. 1):

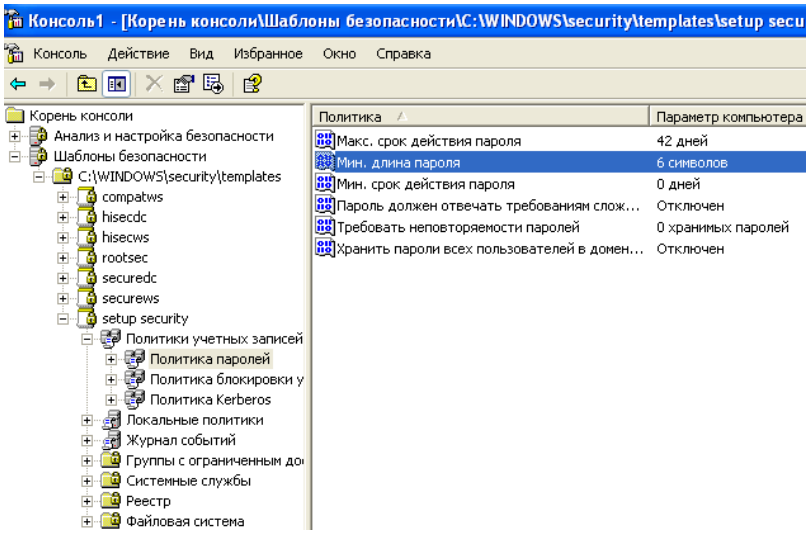
- *Есеп саясаты;*
- *Жергілікті саясаткерлер;*
- *Оқиғалар журналы;*
- *Қол жетімділігі шектеулі топтар;*
- *Жүйелік қызметтер;*
- *Тізілім;*
- *Файлдық жүйе.*



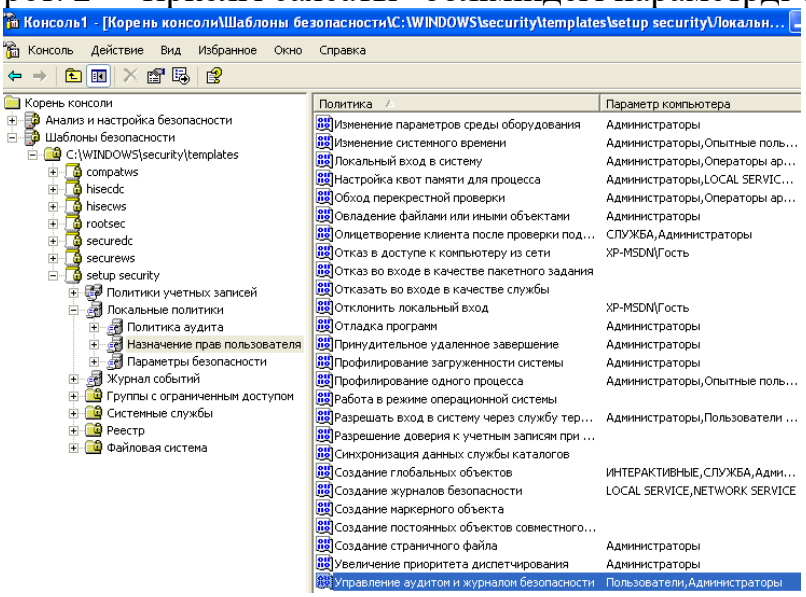
Сурет. 1-Қауіпсіздік үлгісінің құрылымы

Шаблонның құрылымын әрі қарай қарастыру және оның параметрлерін өзгерту "setup security"шаблоны негізінде жүзеге асырылады.

Тіркелгі саясаты және жергілікті саясат бөлімдері ұқсас топтық саясат бөлімдерінің барлық параметрлерін қамтиды. "Тіркелгі саясаты"бөлімінде құпия сөздің ең аз ұзындығының мәнін 6 таңбаға өзгертіңіз -"Пароль саясаты" (сурет. 2). "Жергілікті саясаттар" - "пайдаланушы құқықтарын тағайындау" бөлімінің "аудит және қауіпсіздік журналын басқару" опциясына "пайдаланушылар" тобын қосыңыз (сурет. 3).

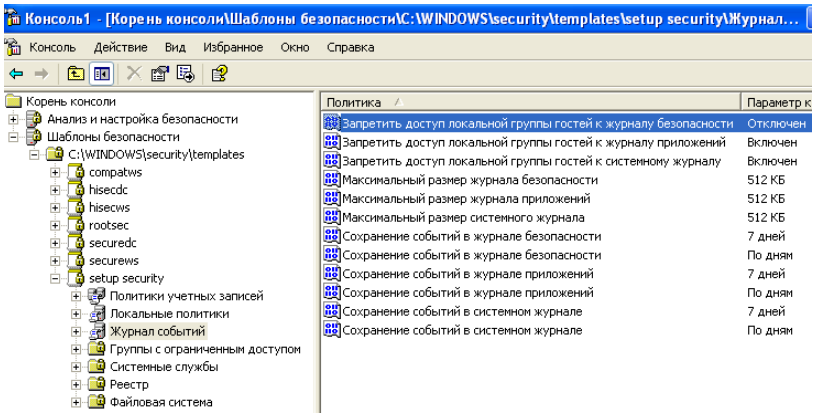


Сурет. 2 - "тіркелгі саясаты" бөліміндегі параметрді өзгерту



Сурет. 3 - "жергілікті саясаттар" бөліміндегі параметрді өзгерту

"Оқиғалар журналы" бөлімі аудит журналдарымен жұмыс істеу ережелерінің параметрлерін қамтиды.Жергілікті қонақтар тобына қауіпсіздік журналына кіруге рұқсат беріңіз (сурет. 4).

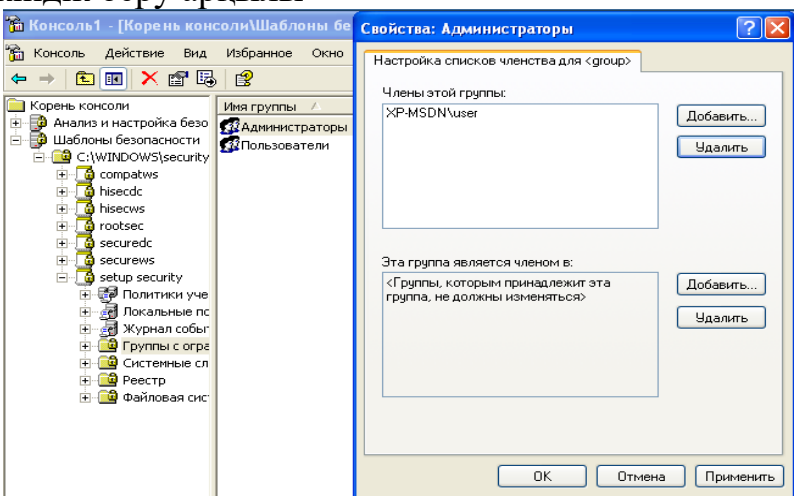


Сурет. 4 - "оқиғалар журналы" бөліміндегі параметрді өзгерту

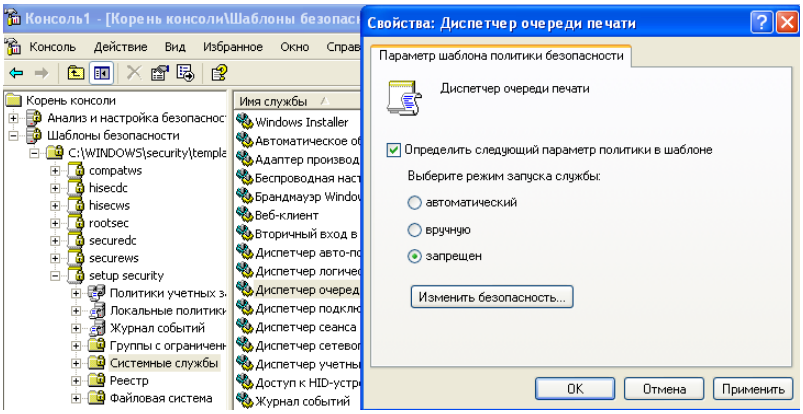
"Шектеулі топтар" бөлімі пайдаланушы топтарының құрамын реттеуге мүмкіндік береді. Мәтінмәндік мәзірді пайдаланып, тізімге "әкімшілер" тобын қосыңыз және топ мүшесі ретінде "пайдаланушы" пайдаланушысын қосыңыз (сурет. 5).

"Жүйелік қызметтер" бөлімінде қызметтерді іске қосу және басқаруға қол жетімділікті шектеу параметрлері бар. "Басып шығару спулері" қызметін іске қосуға тыйым салыңыз (сурет. 6). Бұл қызмет spoolsv деп аталатын процесс ретінде іске қосылады.exe.

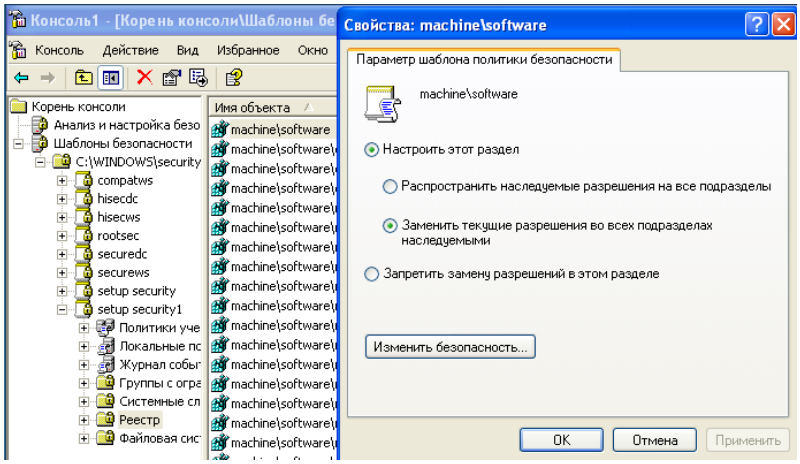
"Тізілім" бөлімінде тізілімнің негізгі тармақтарына кіруді шектеу ережелері бар: бағдарламалық жасақтама, жүйе, пайдаланушылар. HKEY_LOCAL_MACHINE \ SOFTWARE бөліміне кіруді теңшеңіз (сурет. 7) оған топқа толық қол жеткізуге мүмкіндік беру арқылы



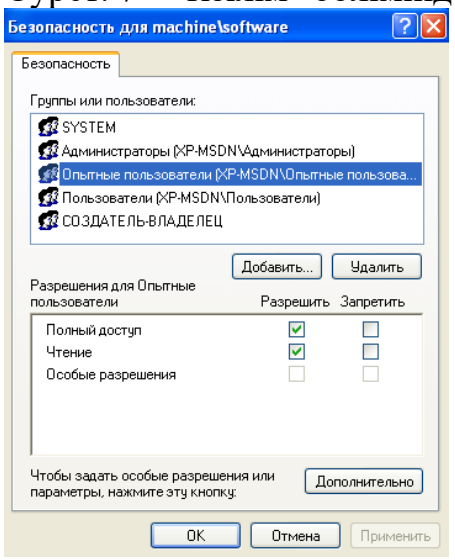
Сурет. 5 - "шектеулі топтар" бөліміндегі параметрді өзгерту



Сурет. 6 - "жүйелік қызметтер" бөліміндегі параметрді өзгерту

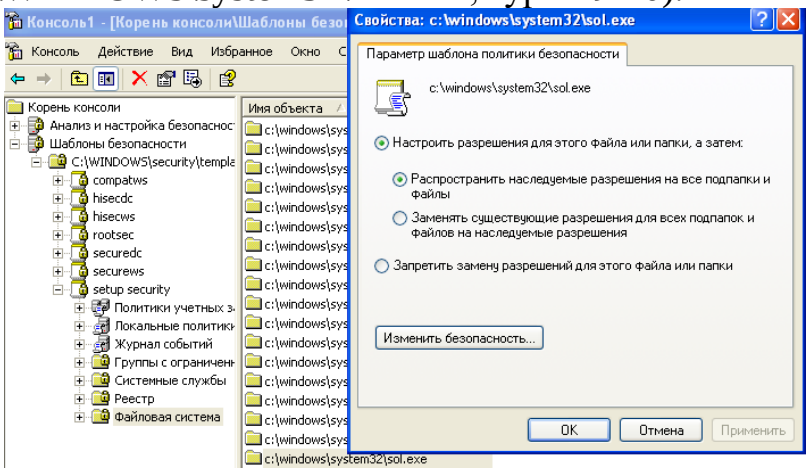


Сурет. 7 - "тізілім" бөліміндегі параметрді өзгерту

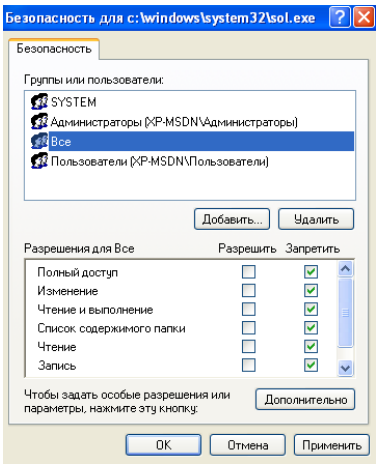


Сурет. 8-тізілім бөліміне кіру құқығын орнату

"Файлдық жүйе" бөлімінде жүйелік дискідегі каталогтарға кіруді шектеу ережелері бар. Барлық пайдаланушыларға "шарфқа" кіруге тыйым салыңыз ("C:\WINDOWS\system32\sol.exe", сурет. 9-10).



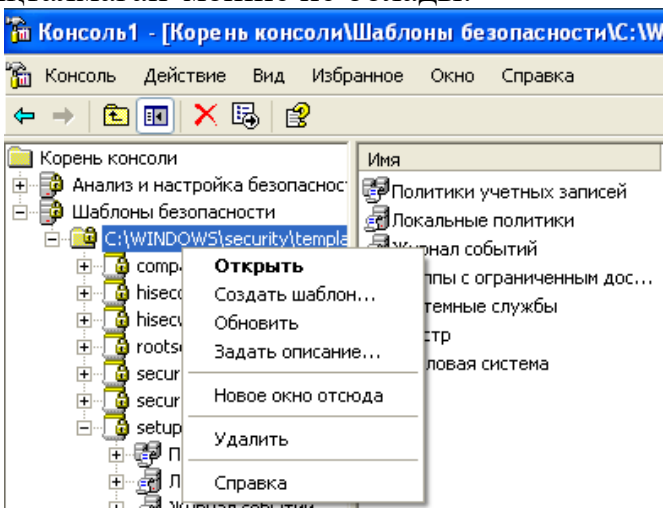
Сурет. 9 - "файлдық жүйе" бөліміндегі параметрді өзгерту



Сурет. 10-файлға кіру құқығын орнату

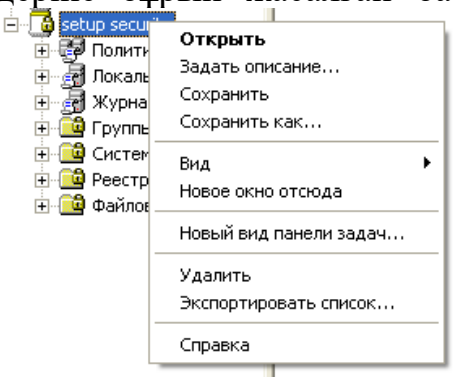
1. Қауіпсіздік үлгілерін басқару

"Қауіпсіздік үлгілері" құралында теңшелетін үлгілерді жасау мүмкіндігі бар. Жаңа үлгіні үлгілері бар каталогтың мәтінмәндік мәзірі арқылы жасауға болады (сурет. 11). Бұл жағдайда шаблон жасалады, онда барлық параметрлер "анықталмаған"мәніне ие болады.



Сурет. 11-жаңа қауіпсіздік үлгісін жасау

Сонымен қатар, өзіңіздің шаблоныңызды бұрыннан бар шаблон негізінде жасауға болады. "Setup security" шаблонының мәтінмәндік мәзіріне қоңырау шалыңыз, "басқаша сақтау" таңдаңыз..."(сурет. 12) және үлгіні жаңа атпен сақтаңыз (мысалы,"test"). Бұл параметр мәндеріне бұрын жасалған барлық өзгерістерді

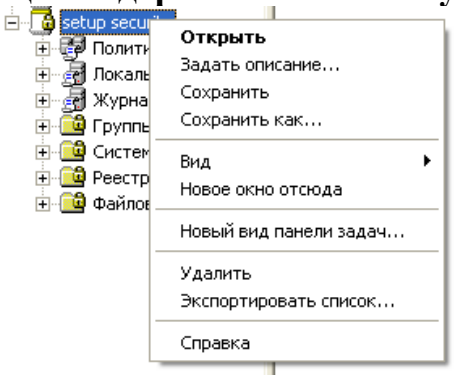


қамтитын жаңа шаблон жасайды.

Сурет. 12-өзгертілген үлгіні сақтау

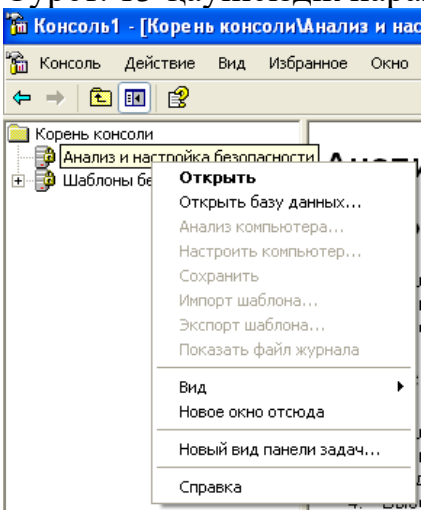
1. Операциялық жүйенің қауіпсіздік параметрлерін талдау

"Қауіпсіздікті талдау және конфигурациялау" мәтінмәндік мәзіріне қоңырау шалыңыз (сурет. 13), "дерекқорды ашу" тармағын таңдаңыз.». Жасалған сілтеме параметрлерінің дерекқорына атау беріңіз. Осыдан кейін сіз қызығушылық үлгісінен параметрлердің мәндерін базаға енгізуіңіз керек.



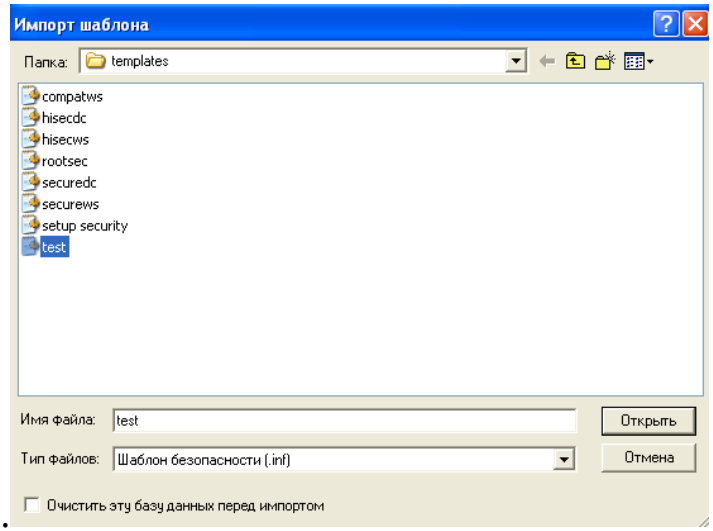
Жасалған үлгіні таңдаңыз (сурет. 14).

Сурет. 13-қауіпсіздік параметрлерінің дерекқорын құру



Сурет. 14-дерекқорға импорттау үшін үлгіні таңдау

Басқа шаблоннан параметрлер базасына енгізу "шаблонды импорттау" мәтінмәндік мәзір пәрмені арқылы мүмкін болады (сурет. 15)

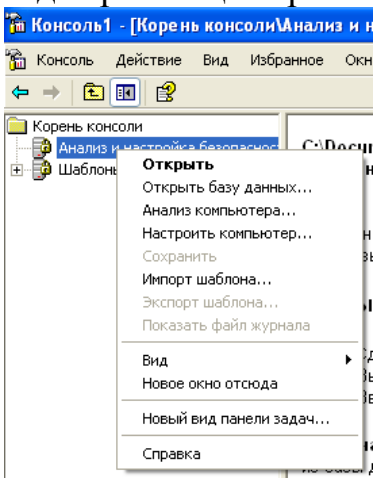


.

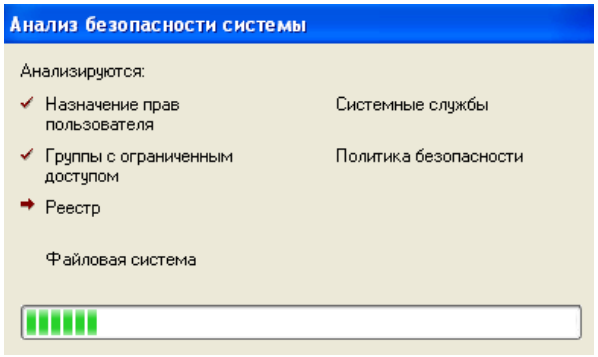
Сурет. 15-үлгіні импорттау

Мәтінмәндік мәзірден " компьютерді талдау."және журнал файлына ұсынылған жолды растаңыз. Осыдан кейін амалдық жүйенің ағымдағы қауіпсіздік параметрлерін талдау басталады (сурет. 16). Талдау нәтижесі қауіпсіздік параметрлерінің ағымдағы (компьютер параметрлері) және анықтамалық (дерекқор параметрі) мәндерін салыстыру болып табылады. Нәтижелерді ұсыну құрылымы шаблон құрылымымен сәйкес келеді (сурет. 17).

Параметрлердің мәндерін салыстыру нәтижелері әр параметрдің атауының жанында орналасқан арнайы белгішелер түрінде ұсынылады (кесте. 1).



Сурет. 16-операциялық жүйенің қауіпсіздік параметрлерін талдау



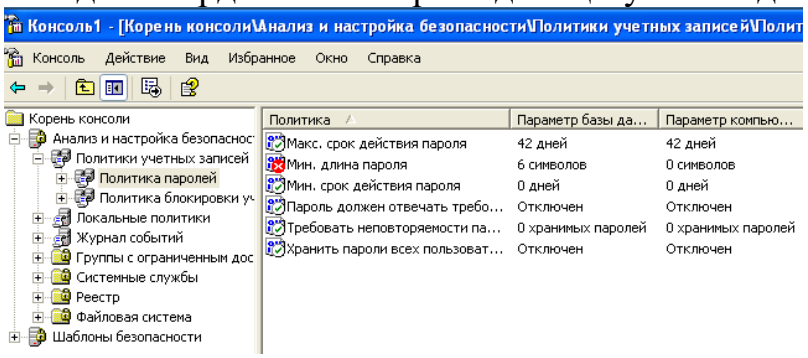
сурет. 17 – операциялық жүйенің қауіпсіздік талдауының нәтижесі

1.Талдау нәтижелері белгішелерінің сипаттамасы

Пиктограмма	***Описание***
	Элемент определён в базе данных анализа и в системе, но значения параметров безопасности не совпадают.
	Элемент определён в базе данных анализа и в системе; значения параметров безопасности совпадают.
	Элемент не анализировался. Возможно, он не был определён в базе данных анализа или пользователь, выполняющий анализ, не имеет достаточных разрешений на анализ данного объекта или области
	Элемент определён в базе данных анализа, однако, не существует в текущей конфигурации системы. Например, может существовать группа с ограниченным доступом, определённая в базе данных анализа и не существующая в анализируемой системе
	Элемент не определён в базе данных анализа или в системе

Жүргізілген талдау нәтижесінде өзгертілген қауіпсіздік параметрлері сәйкес емес деп белгіленгеніне көз жеткізіңіз.

Егер жүйенің ағымдағы параметрлерінің кез-келгені анықтамалыққа қарағанда жақсырақ болса, онда оны базаға енгізуге болады (сурет. 18). Өзгертілген дерекқорды дерекқорды сақтап, "үлгіні экспорттау"тармағын таңдау арқылы мәтінмәндік мәзірден шаблон ретінде сақтауға болады.



Сурет. 18-мәліметтер базасындағы параметрлерді өзгерту

Нәтижесінде "шарфқа" кіруге тыйым салынатын шаблон жасалды, "басып шығару кезегі менеджері" қызметін іске қосуға тыйым салынды және "user" есептік жазбасы бар пайдаланушы "әкімшілер"тобының мүшесі болып табылады. Осы параметрлердің ағымдағы күйін тексеріңіз: "шарфты" іске қосу мүмкіндігі, жұмыс істеп тұрған spoolsv процесі.EXE жылы

"Тапсырмалар менеджері "және" әкімшілер "тобында"пайдаланушы" пайдаланушысының болмауы.

1. Операциялық жүйенің қауіпсіздік параметрлерін орнату

"Қауіпсіздікті талдау және конфигурациялау" мәтінмәндік мәзіріне қоңырау шалып, "компьютерді теңшеу...». Лог-файлға жол расталғаннан кейін амалдық жүйені мәліметтер базасында көрсетілген параметрлердің мәндеріне сәйкес баптау басталады. Сәйкес келмейтін параметрлердің өзгеруін тексеру үшін жүйені қайта талдаңыз. Өзгертілген үлгіде орнатылған параметрлердің қолданылуын тексеріңіз: "шарфты" іске қосып көріңіз, spoolsv процесінің жоқтығын тексеріңіз.тапсырмалар менеджеріндегі exe және "әкімшілер" тобында "user"есептік жазбасының болуы.

Тапсырма

Опцияңызға сәйкес қауіпсіздік үлгісін жасаңыз және жасалған үлгіні пайдаланып амалдық жүйені конфигурациялаңыз.

Вариант 1

Политики учётных записей	Политики учётных записей	Локальные политики
Минимальная длина пароля - 10 символов	Пороговое значение блокировки - 3 ошибки входа	Включите аудит отказов входа в систему

Вариант 2

Локальные политики	Журнал событий	Группы с ограниченным доступом
Запретите группе «Операторы архива» восстановление архивных файлов	Сохранениесобытий в журнале безопасности - вручную	Включите учётную запись «user» в группу «Операторы архива»

Вариант 3

Локальные политики	Журнал событий	Файловая система
Включите аудит доступа к объектам (успех и отказ)	Сохранение событий в журнале безопасности - 30дней	Аудит создания файлов и записи данных (успех и отказ) на каталог C:\Windows и дочерние для учётной записи «user»

Вариант 4

Локальные политики	Локальные политики	Системные службы
Запретите отображение Имени последнего пользователя при входе в систему	Включите обязательное нажатие Ctrl-Alt-Del при входе в систему	Автозапуск службы «Центр обеспечения безопасности»

Вариант 5

Локальные политики	Журнал событий	Группы с ограниченным доступом
Разрешите учётной записи «user» работу с журналомаудита	Максимальный размер журнала безопасности - 2МБ	Включите учётную запись «user» в группу «Опытныепользователи»

Вариант 6

Политики учётных записей	Локальные политики	Системные службы
Включите применение Требований к сложности паролей	Включите аудит управления учётными записями	Автозапуск службы «Автоматическое обновление»

Вариант 7

Локальные политики	Группы с ограниченным доступом	Файловая система

Запретите группе «Пользователи» завершение работы системы	В группу «Пользователи» добавьте пользователя «user» и исключите из неё группы «Интерактивные» и «Прошедшие проверку»	Запретите доступ к редактору реестра группе «Пользователи»

Вариант 8

Политики учётных записей	Локальные политики	Системные службы
Срок действия пароля - 90дней	Запретите учётной записи «user» доступ к компьютеруиз сети	Запретить запуск службы «Диспетчер сеанса справки для удалённогорабочего стола»

Вариант 9

Локальные политики работы системы	Группы с ограниченным доступом «user» и исключите из неё группы «Интерактивные» и «Прошедшие проверку»	Файловая система группе «Пользователи»
Включите очистку файла подкачки при завершении	В группу «Пользователи» добавьте учётную запись	Запретите доступ к оснастке «Службы» (services.msc)

Вариант 10

Локальные политики	Локальные политики	Файловая система
Запретите изменение системного времени группе «Опытные пользователи»	Включите аудит системных событий (успех и отказ)	Запретите учётной записи «user» доступ к оснастке «Просмотр событий»(eventvwr.msc)

Бақылау сұрақтары

1. Windows XP операциялық жүйесінің кіріктірілген құралдарының көмегімен ақпараттық қауіпсіздікке байланысты параметрлердің тұтастығын қалай басқаруға болады?

2. Windows XP кірістірілген құралдарының көмегімен амалдық жүйені қажетті қауіпсіздік параметрлеріне сәйкес конфигурациялауды қалай автоматтандыруға болады?

3. "Қауіпсіздік үлгісі"дегеніміз не?

4. "Қауіпсіздік үлгілері" жабдығы не үшін арналған?

5. Қауіпсіздік үлгісіне қандай параметрлер топтары кіреді?

6. "Қауіпсіздікті талдау және баптау" жабдығы не үшін арналған?

7. Амалдық жүйенің қауіпсіздік параметрлерін талдау кезінде әкімші әрекеттерінің реттілігін сипаттаңыз.

8. Амалдық жүйенің қауіпсіздігін орнату кезінде әкімші әрекеттерінің ретін сипаттаңыз.

9. Операциялық жүйенің қауіпсіздік параметрлерін талдау нәтижелерінің мүмкін түрлерін келтіріңіз.

10. Ағымдағы амалдық жүйенің қауіпсіздік параметрлерін үлгіге қалай енгізуге болады?

Тапсырма

Зертханалық жұмыс туралы есеп әдістемелік нұсқауларда сипатталған стандарт бойынша орындалады