МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ „ЛЬВІВСЬКА ПОЛІТЕХНІКА”

АУДИТ І НАЛАШТУВАННЯ БЕЗПЕКИ У WINDOWS XP

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторних робіт
з дисципліни „Адміністрування та безпека комп’ютерів”
для студентів спеціальності
7.080403 „Програмне забезпечення автоматизованих систем”

Затверджено
на засіданні кафедри
програмного забезпечення
Протокол № 10 від 19.04.2007 р.

Львів – 2007

Аудит і налаштування безпеки у Windows XP: Методичні вказівки до виконання лабораторних робіт з дисципліни „Адміністрування та безпека комп'ютерів" для студентів спеціальності „Програмне забезпечення автоматизованих систем" / Укл.: В.С. Яковина, О.Є. Білас – Львів: Видавництво Національного університету „Львівська політехніка", 2007. – 43 с.

Укладачі Яковина В.С., канд. фіз.-мат. наук, доц.
Білас О.Є., канд. техн. наук, доц.

Відповідальний за випуск Федасюк Д.В., д-р тех. наук, проф.

Рецензенти Федорчук Є.Н., канд. тех. наук, доц.
Фечан А.В., канд. фіз.-мат. наук, доц.

Лабораторна робота № 1.
РЕАЛІЗАЦІЯ МЕХАНІЗМУ ГРУПОВИХ ПОЛІТИК У WINDOWS XP. АНАЛІЗ І НАЛАШТУВАННЯ БЕЗПЕКИ.

Мета роботи: Ознайомлення зі структурою, принципом роботи та налаштуванням об’єкта групової політики на локальному комп’ютері під управлінням ОС Windows XP. Навчитись використовувати та створювати шаблони безпеки для ефективного налаштування та аналізу типових параметрів безпеки.

Теоретичні відомості.

Групова політика – це технологія управління, що використовується для налаштування параметрів конфігурації робочих столів для груп комп’ютерів і користувачів. Групові політики можуть включати в себе параметри безпеки, параметри установки та підтримки програмного забезпечення і параметри для скриптів (сценаріїв), що управляють процесами завантаження і завершення роботи з системою. Групові політики зберігаються у вигляді об’єктів Group Policy (GPO), які, своєю чергою, зв’язуються з об’єктами Active Directory – сайтами, доменами чи організаційними одиницями (OU), крім того існує об’єкт локальної групової політики комп’ютера[1].

Численні параметри, що визначаються в рамках об'єкту групової політики, розділено на дві частини. Одна частина параметрів використовується для конфігурації комп'ютера (computer configuration), інша частина параметрів використовується для конфігурації середовища користувача (user configuration). Конфігурація комп'ютера припускає визначення значень для параметрів, що впливають на формування оточення будь-яких користувачів, що реєструються на заданому комп'ютері. Конфігурація середовища користувача дає можливість управляти процесом формування оточення конкретного користувача, незалежно від того, на якому комп'ютері він реєструється в мережі.

Незалежно від типу конфігурації, параметри групової політики організовані в спеціальні категорії (рис. 1). Кожна з категорій параметрів групової політики визначає окрему область оточення користувача. Доступні категорії параметрів перераховані в табл. 1. Перераховані в таблиці категорії параметрів надають адміністратору доступ до різних механізмів конфігурації

[1] GPO, який застосовується локально, зберігається в локальній папці комп’ютера %systemroot%\system32\GroupPolicy. Комп’ютер може мати тільки одну локальну групову політику.

робочих станцій. У свою чергу категорії параметрів групової політики організовані в три контейнери відповідно до свого призначення:

- **Software Settings** (Конфігурація програм). У контейнері розміщуються категорії параметрів групової політики, за допомогою яких можна управляти переліком додатків, доступних користувачам;
- **Windows Settings** (Конфігурація Windows). У контейнері розміщуються категорії параметрів групової політики, що визначають налаштування безпосередньо самої операційної системи. Вміст цього контейнера може бути різним, залежно від того, на якому рівні визначаються параметри групової політики (для користувача або комп'ютера);
- **Administrative Templates** (Адміністративні шаблони). Цей контейнер містить категорії параметрів групової політики, які встановлюють правила на основі системного реєстру[1].

Всі компоненти групової політики можна редагувати за допомогою Group Policy Editor.

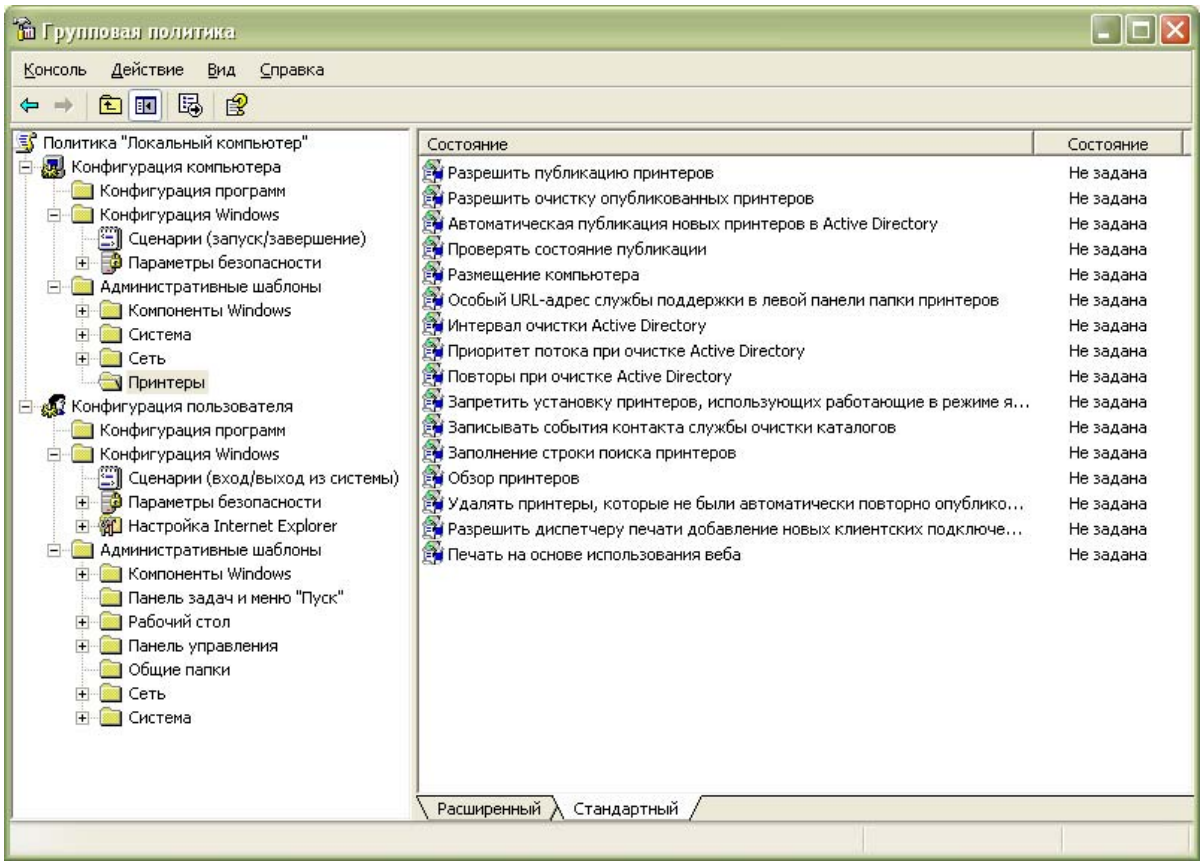


Рис. 1. Структура об'єкту групової політики.

[1] Адміністративний шаблон є текстовим файлом у форматі Unicode, який містить перелік ключів і параметрів реєстру. Такі файли мають розширення .adm і зберігаються в папці %SystemRoot%\inf.

Таблиця 1

Категорії параметрів групової політики

Категорія	Контейнер	Опис
Software Installation	Software Settings	Ця категорія параметрів використовується для централізованого управління додатками, доступними на певному комп'ютері, або для певного користувача. При цьому залежно від параметрів групової політики додатки можуть або встановлюватися примусово, або рекомендуватися для установки.
Remote Installation Service	Windows Settings	Ця категорія параметрів використовується для управління процесом віддаленої установки на клієнтському комп'ютері. Ця категорія параметрів доступна тільки у випадку конфігурації на рівні користувача.
Scripts	Windows Settings	Категорія використовується для визначення сценаріїв, які виконуватимуться при включенні/виключенні комп'ютера (Startup/Shutdown Scripts), або при реєстрації користувача в системі чи його виході з неї (Logon/Logoff Scripts).
Security Settings	Windows Settings	Параметри цієї категорії використовуються для управління налаштуваннями безпеки клієнтського комп'ютера. Крім групової політики, адміністратор може також використовувати інші механізми для управління налаштуваннями безпеки.
Folder Redirection	Windows Settings	За допомогою параметрів цієї категорії адміністратор може налаштовувати процес перенаправлення папок з призначеного для користувача профілю (таких, наприклад, як My Documents) на деякий мережний ресурс. Ця категорія параметрів доступна тільки для конфігурації користувача.
Internet Explorer Maintenance	Windows Settings	Параметри цієї категорії використовуються для налаштування браузера Internet Explorer. Ця категорія параметрів доступна тільки для конфігурації користувача.

Windows Components	Administrative Templates	У цій категорії представлені параметри, за допомогою яких адміністратор може здійснювати управління налаштуваннями Windows-компонентів, встановлених на системі, що налаштовується.
Start Menu and Taskbar	Administrative Templates	Параметри цієї категорії дозволяють адміністратору налаштовувати головне меню і панель завдань клієнтського комп'ютера (насамперед, обмежувати доступну функціональність). Ця категорія параметрів доступна тільки для конфігурації користувача.
Desktop	Administrative Templates	Параметри цієї категорії дозволяють адміністратору налаштовувати вигляд робочого столу клієнтського комп'ютера і його функціональність. Ця категорія параметрів доступна тільки для конфігурації користувача.
Control Panel	Administrative Templates	Параметри цієї категорії дозволяють адміністратору управляти відображенням окремих компонентів панелі управління на клієнтському комп'ютері. Ця категорія параметрів доступна тільки для конфігурації користувача.
Shared Folders	Administrative Templates	Параметри цієї категорії дозволяють управляти процесом публікації загальних папок. Ця категорія параметрів доступна тільки для конфігурації користувача.
Networks	Administrative Templates	Ця категорія параметрів використовується для управління конфігурацією мережних компонентів системи.
System	Administrative Templates	У даній категорії представлені параметри, що дозволяють управляти настройками реєстру, що впливають на поведінку системи в цілому
Printers	Administrative Templates	Параметри цієї категорії використовуються для управління процесом публікації принтерів. Ця категорія параметрів доступна тільки для конфігурації комп'ютера.

Побудова ієрархії об'єктів групової політики. Параметри, визначені в рамках об'єкту групової політики, впливають тільки на ті об'єкти каталога, до яких вони застосовані. Щоб визначити множину об'єктів каталога, що підпадають під дію того або іншого об'єкту групової політики, необхідно виконати прив'язку останнього до одного або декількох контейнерів каталога. Для будь-якого об'єкту групової політики (за винятком локальних)

дозволяється прив'язка до будь-якого з трьох класів об'єктів каталога – сайту, домена або підрозділу. Будь-які об'єкти, асоційовані з обліковими записами користувачів і комп'ютерів, що розташовуються всередині цих контейнерів, підпадають під дію прив'язаного об'єкту групової політики.

У випадку, коли в рамках дерева каталога є прив'язка декількох об'єктів групової політики, цілком можлива ситуація, коли деякі об'єкти каталога (або навіть всі) можуть підпадати під дію відразу декількох об'єктів групової політики. При цьому параметри, визначені в них, застосовуються до об'єктів каталога відповідно до певного порядку:

- спочатку застосовуються об'єкти групової політики, прив'язані до сайту, в якому знаходиться об'єкт каталога;
- після цього застосовуються об'єкти, прив'язані на рівні домена;
- останніми застосовуються об'єкти групової політики, прив'язані до організаційних одиниць.

Якщо є декілька вкладених організаційних одиниць, об'єкти групової політики застосовуються відповідно до рівнів вкладеності. В такому випадку йдеться про успадкування параметрів об'єктів вищого рівня групової політики (group policy inheritance).

Об'єкти групової політики, прив'язані до дочірніх контейнерів, можуть перевизначати параметри об'єктів групової політики, прив'язаних до об'єктів вищого рівня. В цьому випадку прийнято говорити про перевизначення (group policy overriding) параметрів об'єкту групової політики. При цьому успадковуються тільки ті параметри об'єктів групової політики, що були визначені для батьківського контейнера, але не визначені для дочірнього. Інакше значення параметрів, визначені в об'єкті групової політики, прив'язаному до об'єкту нижчого рівня групової політики, перевизначатимуть значення аналогічних параметрів об'єкту групової політики, прив'язаної до контейнера вищого рівня. Якщо деякий параметр об'єкту групової політики допускає безліч значень, значення параметра об'єкту групової політики батьківського контейнера доповнюють значення аналогічного параметра, визначеного в рамках об'єкту групової політики дочірнього контейнера.

Оснащення "Шаблони безпеки". За допомогою оснащення "Шаблони безпеки" можна створити політику безпеки для комп'ютера або мережі. Використовуючи це єдине оснащення, можна управляти всією безпекою системи. Оснащення "Шаблони безпеки" не надає нових параметрів безпеки, а просто впорядковує і надає зручний доступ до всіх наявних атрибутів безпеки для спрощення адміністрування.

При імпорті шаблону безпеки в об'єкт групової політики полегшується адміністрування домена, оскільки безпека настроюється для домена або підрозділу тільки один раз.

Щоб застосувати шаблон безпеки на локальному комп'ютері, можна використовувати засіб "Аналіз і настройка безпеки".

Шаблони безпеки можна використовувати, щоб визначити перелічені в табл. 2 елементи.

Таблиця 2

Елементи шаблонів безпеки

Область безпеки	**Опис**
Політики облікових записів	Політика паролів, політика блокування облікового запису і політика Kerberos
Локальні політики	Політика аудиту, призначення прав користувачів і параметри безпеки
Журнал подій	Параметри журналів подій додатків, системних подій і подій безпеки
Групи з обмеженим доступом	Участь в групах безпеки
Системні служби	Запуск і дозволи для системних служб
Реєстр	Дозволи для розділів реєстру
Файлова система	Дозволи для файлів і папок

Всі шаблони зберігаються в текстових файлах з розширенням .inf. Це дозволяє копіювати, вставляти, імпортувати і експортувати будь-які атрибути шаблону. У шаблоні безпеки можуть зберігатися всі атрибути безпеки, за виключенням політик безпеки IP і політик відкритого ключа.

Нові і готові шаблони

Можна створювати шаблони безпеки, що відповідають вимогам користувача, або використовувати готові шаблони. Перед зміною параметрів безпеки необхідно визначити параметри безпеки системи, що використовуються за умовчанням, а також їх призначення.

Існує декілька готових шаблонів, які рекомендується використовувати для захисту системи залежно від потреб конкретного користувача. Ці шаблони використовуються для виконання наступних дій:

- Відновлення параметрів за умовчанням (Setup security.inf);
- Впровадження середовища підвищеного захисту (Hisecws.inf);
- Впровадження середовища з нижчим рівнем захисту, але з більшою сумісністю (Compatws.inf);

- Захист кореневого каталога системи (Rootsec.inf);

Готові шаблони безпеки

Готові шаблони безпеки[1] є відправною точкою в створенні політик безпеки, які налаштовуються для задоволення вимог організації. Після налаштування готових шаблонів безпеки ці шаблони можна використовувати для зміни конфігурації одного комп'ютера або безлічі комп'ютерів[2]. Змінити конфігурацію комп'ютерів можна за допомогою оснащення "Аналіз і настройка безпеки", утиліти командного рядка Secedit.exe, а також за допомогою імпорту шаблону в оснащення "Локальна політика безпеки". Можна змінювати конфігурацію декількох комп'ютерів, імпортувавши шаблон в компонент "Параметри безпеки", що є розширенням оснащення "Групова політика". На основі шаблонів безпеки можна також виконувати аналіз можливих слабких місць безпеки і порушень політики системи за допомогою оснащення "Аналіз і настройка безпеки". За умовчанням готові шаблони безпеки збережені в розташуванні: %systemroot%\Security\Templates

- **Безпека за умовчанням (Setup security.inf)**

Шаблон Setup security.inf є шаблоном для конкретного комп'ютера і містить параметри безпеки, використовувані за умовчанням, які застосовуються під час установки операційної системи, включаючи дозволи для файлів кореневого каталога системного диска. Цей шаблон можна використовувати повністю або частково з метою аварійного відновлення. Шаблон Setup security.inf не можна застосовувати за допомогою оснащення "Групова політика".

- **Сумісний (Compatws.inf)**

Дозволи за умовчанням для робочих станцій і серверів спочатку створюються для їх локальних груп: "Адміністратори", "Досвідчені користувачі" і "Користувачі". Члени групи "Адміністратори" володіють найбільшими правами тоді як члени групи "Користувачі" – якнайменшими. З цієї причини можна значно підвищити безпеку, надійність і понизити загальну вартість володіння системою, якщо дотримуватися наступних правил:

  - переконатися, що кінцеві користувачі є членами групи "Користувачі";
  - упровадити додатки, які можуть успішно запускатися і виконуватися членами групи "Користувачі".

[1] Ці шаблони призначені для комп'ютерів, на яких використовуються параметри безпеки за умовчанням. Іншими словами, будучи встановленими на комп'ютері, ці шаблони значно змінюють стандартні параметри безпеки. Але вони ***не*** встановлюють стандартні параметри безпеки, перш ніж змінити їх.

[2] Забезпечення безпеки неможливе в системах Windows XP Professional, встановлених на дисках з файловою системою FAT.

Особи, що мають права групи "Користувачі", можуть успішно працювати із додатками, сертифікованими для Windows. Проте такі користувачі швидше за все не зможуть запускати не сертифіковані для Windows додатки. Якщо необхідно забезпечити підтримку не сертифікованих додатків, існують дві можливості:

- Всі члени групи "Користувачі" повинні також бути членами групи "Досвідчені користувачі".
- Використовувати додаткові дозволи за умовчанням, створені для групи "Користувачі".

Оскільки члени групи "Досвідчені користувачі" володіють успадкованими можливостями, такими як створення користувачів, груп, принтерів і загальних ресурсів, деякі адміністратори вважають за краще надати додаткові дозволи групі "Користувачі", замість зарахування кінцевих користувачів в групу "Досвідчені користувачі". Для цих цілей служить "Сумісний" шаблон. За допомогою цього шаблону змінюються дозволи для файлів і реєстру, використовувані за умовчанням, створені для групи "Користувачі", які відповідають вимогам більшості не сертифікованих застосувань. Крім того, оскільки після застосування сумісного шаблону користувачі не повинні приєднуватися до групи "Досвідчені користувачі", всі члени групи "Досвідчені користувачі" віддаляються.

Сумісний шаблон не слід застосовувати до комп'ютерів, які є контролерами домена. Наприклад, не слід імпортувати сумісний шаблон в стандартний домен або в об'єкт групової політики стандартного контролера домена.

- **Захист (Secure*.inf)**

У шаблоні "Захист" визначаються параметри підвищеної безпеки. Найменш імовірно, що вони впливають на сумісність. Наприклад, в шаблоні "Захист" визначаються параметри надійних паролів, блокування і аудиту.

Крім цього, шаблоном "Захист" обмежується використання LAN Manager і протоколів перевірки достовірності NTLM шляхом налаштування клієнтів на відправку відповідей у форматі NTLMv2.

Шаблони безпеки також визначають додаткові обмеження для анонімних користувачів та включають підписування пакетів SMB на сервері, яке за умовчанням відключено для робочих станцій і серверів.

- **Підвищений захист (hisec*.inf)**

Група шаблонів підвищеного захисту включає шаблони, що накладають додаткові обмеження на рівні шифрування і підпису, необхідні для перевірки достовірності і для даних, що передаються по безпечним каналам між клієнтами SMB і серверами. Наприклад, тоді як параметри шаблонів безпеки

визначають відмову серверів від відповідей LAN Manager, параметри шаблонів підвищеного захисту визначають відмову серверів як від відповідей LAN Manager, так і від відповідей NTLM. Шаблон захисту включає підписання пакетів SMB на сервері, а для шаблону підвищеного захисту таке підписання є необхідним. Для шаблонів підвищеного захисту є необхідним надійне кодування і підпис для даних, що передаються по безпечному каналу між доменом і членом домена і між двома доменами, між якими встановлені довірчі відносини.

Крім обмежень на використання протоколів LAN Manager і вимог шифрування і підпису даних SMB і потоку даних безпечного каналу шаблони підвищеного захисту також обмежують використання кешованих даних входу в систему, таких як дані, збережені за допомогою Winlogon і засобу "Збереження імен користувачів і паролів".

Крім цього, в шаблоні Hisecws параметри групи обмеженого доступу використовуються для виконання наступних дій:

- Видалення всіх членів групи "Досвідчені користувачі".
- Перевірка того, що тільки адміністратори домена і локальні облікові записи адміністратора є членами локальної групи "Адміністратори".

Шаблоном Hisecws визначаються ці обмеження для груп при виконанні тільки сертифікованих для Windows 2000 додатків. При роботі тільки з сертифікованими додатками ані небезпечні сумісні шаблони, ані небезпечна група "Досвідчені користувачі" не є необхідними. Користувачі можуть успішно працювати з сертифікованими додатками в безпечному контексті звичного користувача, який визначається параметрами безпеки за умовчанням файлової системи і реєстру.

- **Безпека системного кореневого каталога (Rootsec.inf)**

Шаблоном Rootsec.inf визначаються нові дозволи для кореневого каталога Windows XP Professional. За умовчанням ці дозволи визначаються шаблоном Rootsec.inf для кореневого каталога системного диска. Цей шаблон можна використовувати, щоб повторно застосувати дозволи для кореневого каталога, якщо вони були випадково змінені. Шаблон також може бути змінений для застосування цих дозволів для кореневого каталога до інших томів. Шаблоном не перевизначаються явні дозволи, визначені для всіх дочірніх об'єктів. Шаблоном розповсюджуються тільки успадковані дочірніми об'єктами дозволи.

- **Відсутність SID користувача серверу терміналів (Notssid.inf)**

Стандартні таблиці управління доступом до файлової системи і реєстру, розташовані на серверах, надають дозволи для SID (Secuity ID) сервера терміналів. SID сервера терміналів використовується, тільки якщо цей сервер

запущений в режимі сумісності додатків. Якщо сервер терміналів не використовується, цей шаблон може бути застосований для видалення непотрібних SID сервера терміналів з файлової системи і реєстру. Проте видалення запису управління доступом для SID сервера терміналів з файлової системи і реєстру не підвищує безпеку системи. Замість видалення SID сервера терміналів слід запустити сервер терміналів в режимі повної безпеки. При роботі в режимі повної безпеки SID сервера терміналів не використовується.

Щоб імпортувати[1] шаблон безпеки:

1. Відкрийте оснащення "Аналіз і настройка безпеки".
2. У дереві консолі клацніть правою кнопкою миші вузол "Аналіз і настройка безпеки" і виберіть команду "Імпорт шаблону".
3. (Необов'язково) Для видалення з бази даних від всіх збережених раніше шаблонів встановіть відмітку "Очистити цю базу даних перед імпортом".
4. Клацніть файл шаблону і натисніть кнопку "Відкрити".
5. Повторіть попередній крок для всіх шаблонів, для яких вимагається виконати злиття з базою даних.

Щоб виконати аналіз безпеки системи:

1. Відкрийте оснащення "Аналіз і настройка безпеки".
2. У дереві консолі клацніть правою кнопкою миші вузол "Аналіз і настройка безпеки" і виберіть команду "Відкрити базу" даних.
3. У діалоговому вікні "Відкрити базу" даних виконайте одну з наступних дій:
   - щоб створити нову базу даних, введіть ім'я в полі "Ім'я файлу" і натисніть кнопку "Відкрити";
   - щоб відкрити існуючу базу даних, виберіть базу даних і натисніть кнопку "Відкрити".
4. Якщо створюється нова база даних, в діалоговому вікні "Імпорт шаблону" виберіть шаблон і натисніть кнопку "Відкрити".
5. У області відомостей клацніть правою кнопкою миші вузол "Аналіз і настройка безпеки" і виберіть команду "Аналіз комп'ютера".
6. Виконайте одну з наступних дій:
   - для використання стандартного журналу в групі "Шлях файлу журналу помилок" натисніть кнопку "ОК";

[1] Імпорт шаблонів в особисту базу даних впливає тільки на базу даних аналізу і не змінює параметри системи.

- для вибору іншого журналу введіть в полі "Шлях файлу журналу помилок" допустимі шлях і ім'я файлу.

Щоб налаштувати безпеку системи:

1. Відкрийте оснащення "Аналіз і настройка безпеки".
2. У дереві консолі клацніть правою кнопкою миші вузол "**Аналіз і настройка безпеки"** і виберіть команду "**Відкрити базу** даних".
3. У діалоговому вікні "**Відкрити базу** даних" виконайте одну з наступних дій:
   - щоб створити нову базу даних, введіть ім'я в полі "**Ім'я файлу"** і натисніть кнопку "**Відкрити"**;
   - щоб відкрити існуючу базу даних, виберіть базу даних і натисніть кнопку "**Відкрити"**.
4. Якщо створюється нова база даних, в діалоговому вікні "**Імпорт шаблону"** виберіть шаблон і натисніть кнопку "**Відкрити"**.
5. У дереві консолі клацніть правою кнопкою миші вузол "**Аналіз і настройка безпеки"** і виберіть команду "**Налаштувати комп'ютер"**.
6. Виконайте одну з наступних дій:
   - для використання стандартного журналу в групі "**Шлях файлу журналу помилок"** натисніть кнопку "**ОК"**;
   - для вибору іншого журналу введіть в полі "**Шлях файлу журналу помилок"** допустимі шлях і ім'я файлу.

Завдання до виконання роботи

1. Відкрити оснастку mmc "Групповая политика" (в ОС Windows XP SP2 – "Редактор объекта групповой политики"). Перейти в гілку "Политика паролей" (рис. 2), задати мінімальну довжину пароля (рис. 3). Після цього спробувати змінити власний пароль на такий, довжина якого менша за вказану в політиці, переконатись в неможливості такої дії (рис. 4). Повторити такі дії з параметрами "Пароль должен отвечать требованиям сложности" та "Требовать неповторяемости паролей".

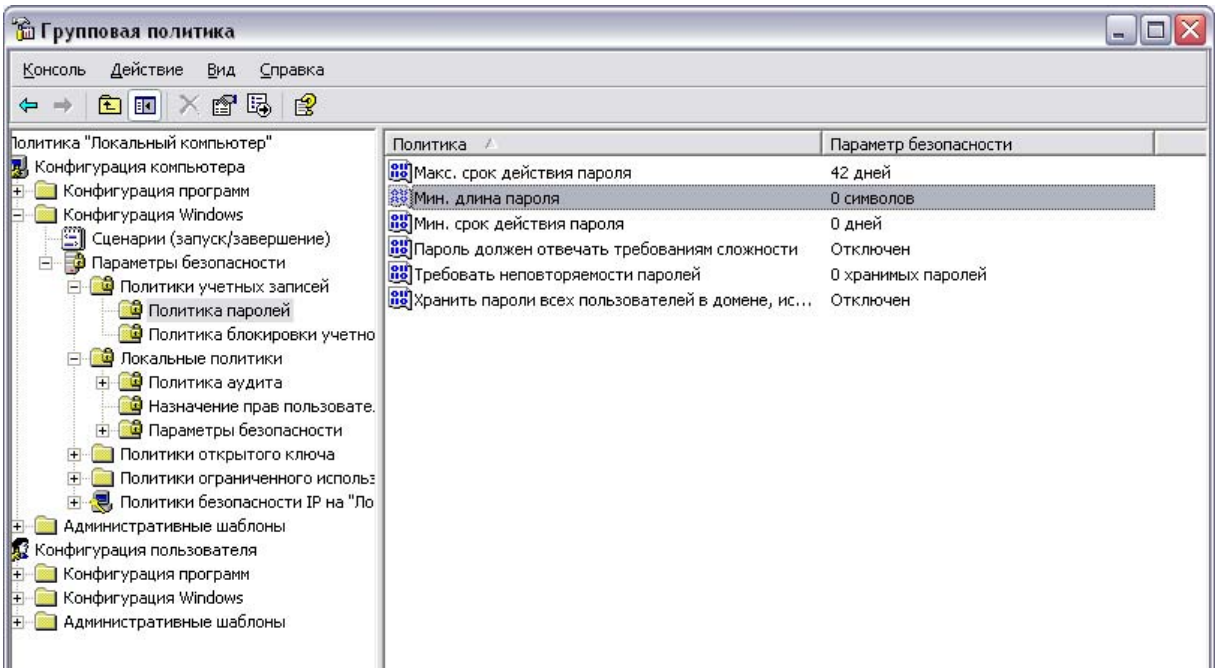


Рис. 2. Оснащення "Групова політика".

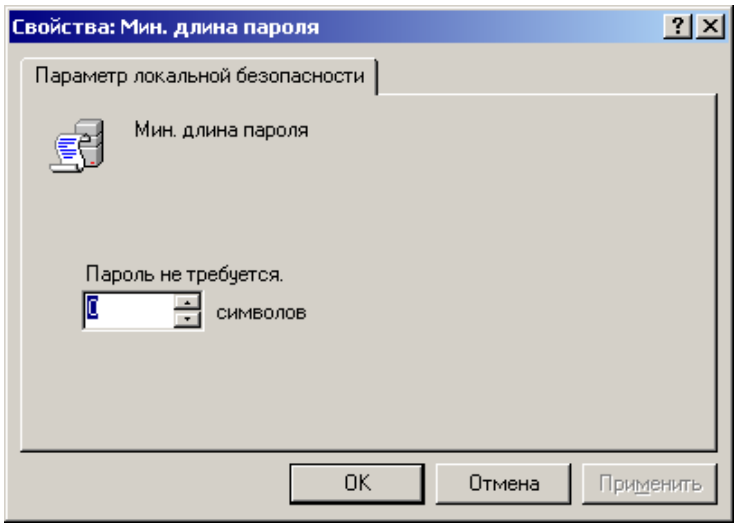


Рис. 3. Властивості параметру безпеки.

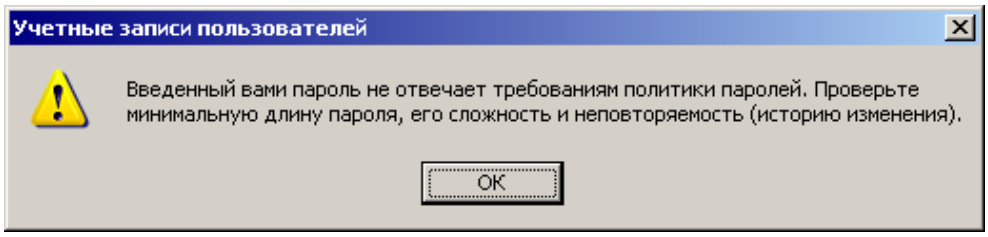


Рис. 4. Повідомлення системи про невідповідність параметру значенню політики.

2. Перейти в гілку "Политика блокировки учетной записи" (рис. 2), задати граничне значення блокування (рис. 5). Після цього спробувати декілька разів зайти в систему з неправильним вводом пароля – переконатись у спрацюванні блокування (рис. 6). Увійти в систему як адміністратор – зняти блокування вручну з оснастки "Локальные пользователи и группы" у властивостях заблокованого облікового запису (рис. 7).

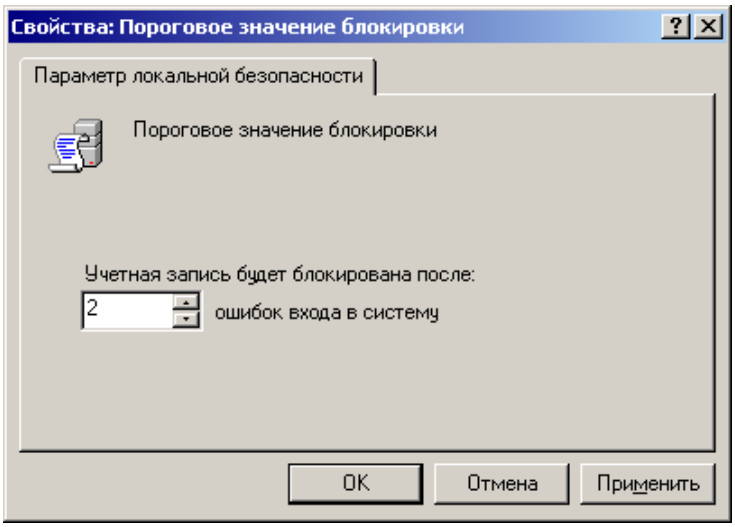


Рис. 5. Встановлення граничного значення блокування облікового запису.

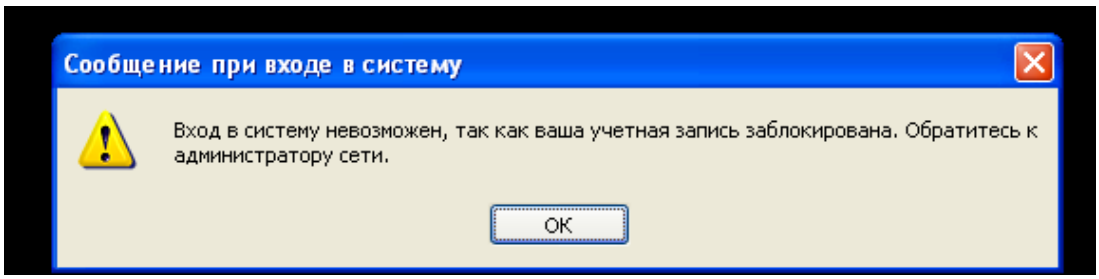


Рис. 6. Повідомлення системи про блокування облікового запису.

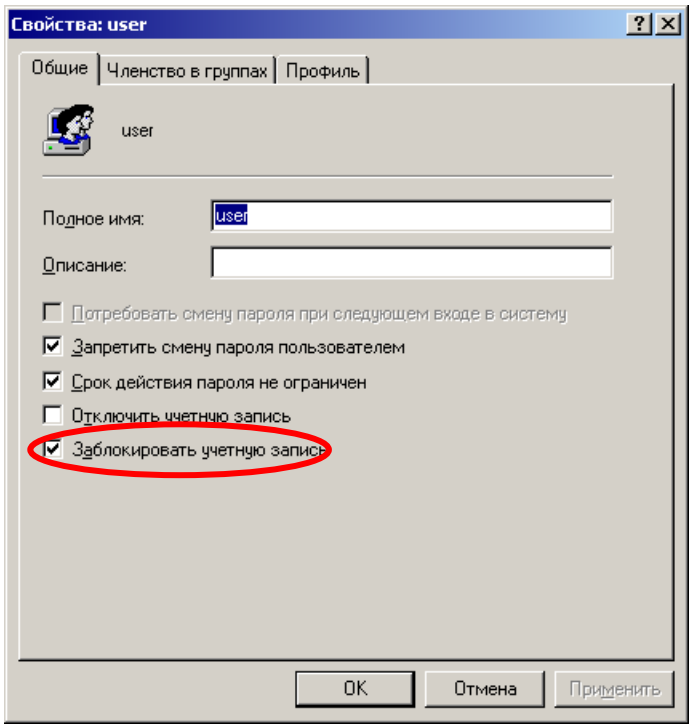


Рис. 7. Властивості заблокованого облікового запису.

3. Налаштування привілеїв користувачів. Перейти в гілку "Локальные политики | Назначение прав пользователя" (рис. 8), задати привілей на вимкнення комп'ютера тільки для групи адміністраторів (рис. 9). Увійти до системи як користувач без адміністративних привілеїв; переконатись, що пункт "Выключить компьютер" зник з меню "Пуск", крім того завершення роботи системи з командного рядка теж неможливе (рис. 10).

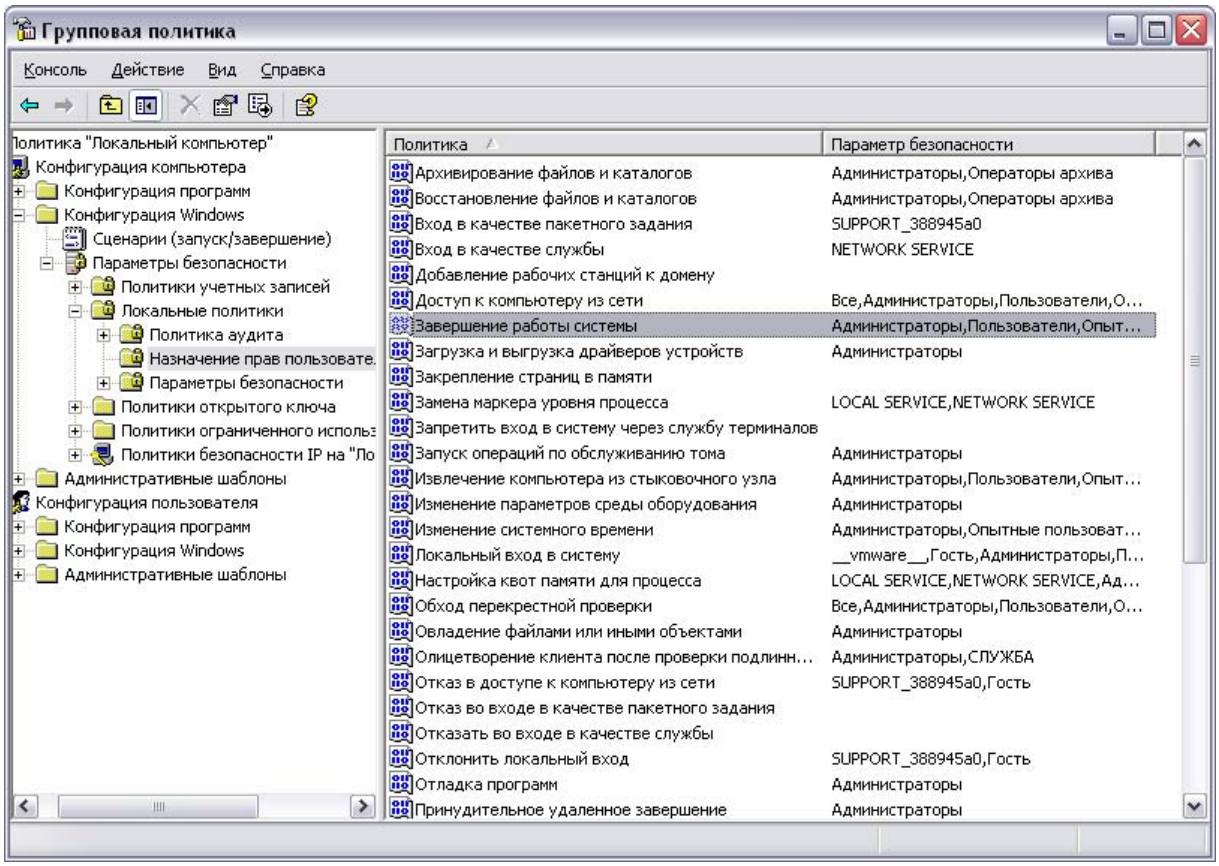


Рис. 8. Призначення прав користувачів за допомогою групової політики.

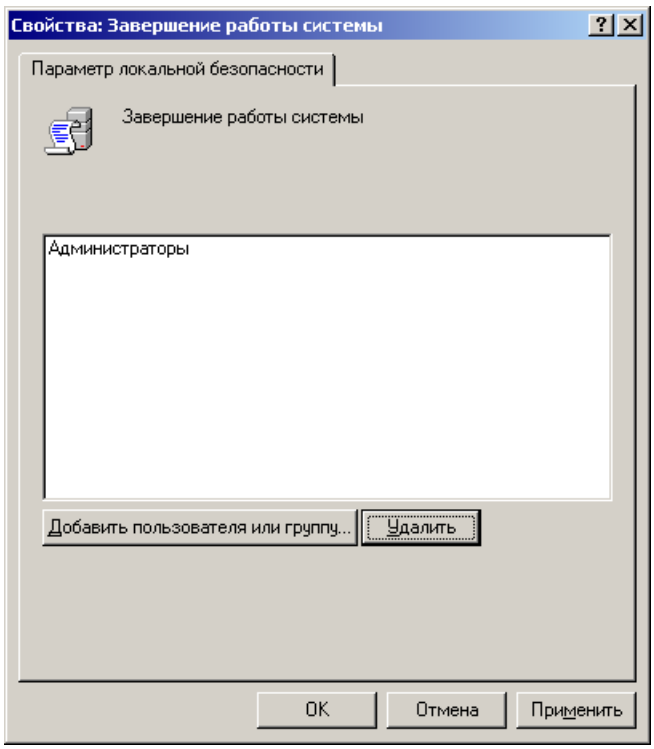


Рис. 9. Властивості параметру прав користувачів на завершення роботи системи.

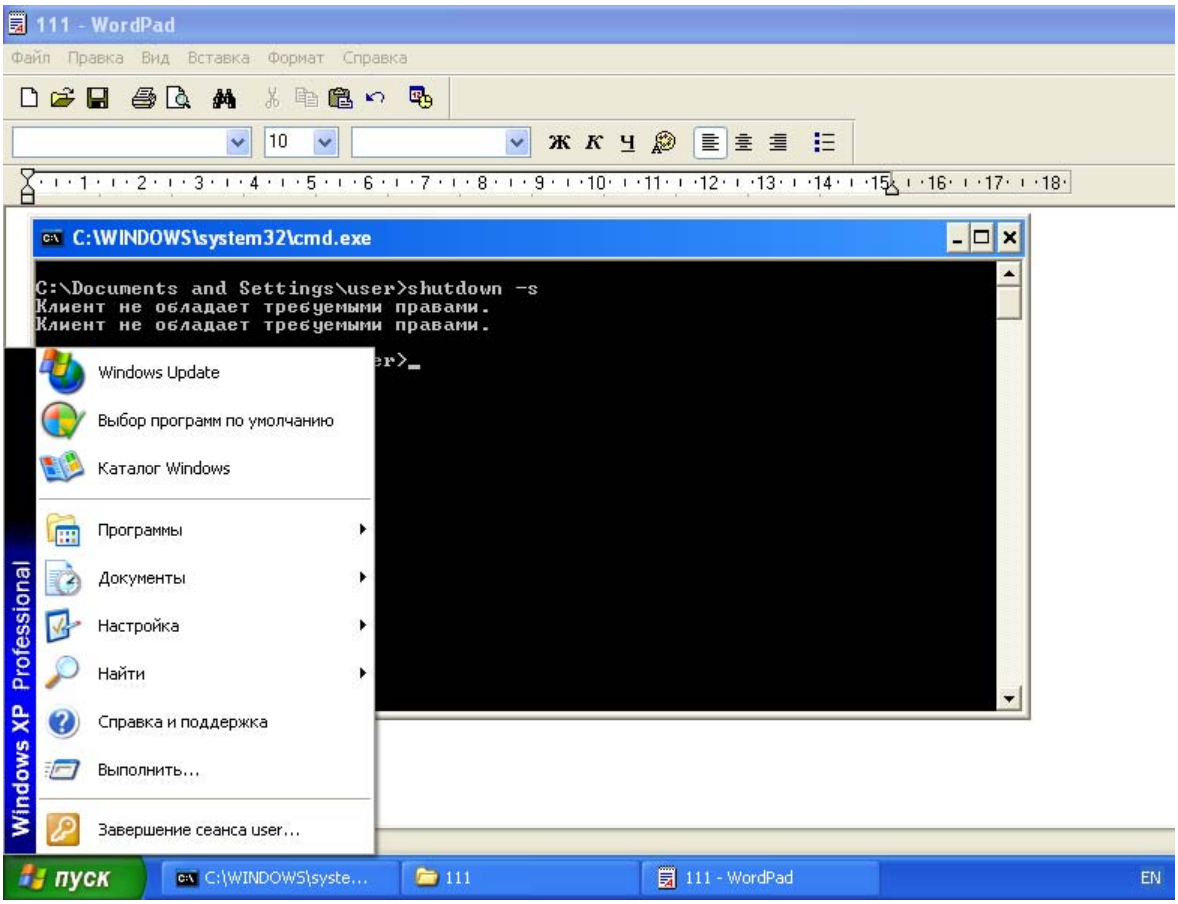


Рис. 10. Результат виконання політики стосовно заборони користувачу завершення роботи системи.

4. Оглянути вміст гілки "Административные шаблоны" як для частини "Конфигурация компьютера", так і "Конфигурация пользователя". В гілці "Панель управления | Экран" увімкнути політику видалення значка "Екран" з панелі управління (рис. 11). Спробувати змінити параметри екрану (рис. 12). Переконатись, що політики діють на усіх користувачів локальної системи.

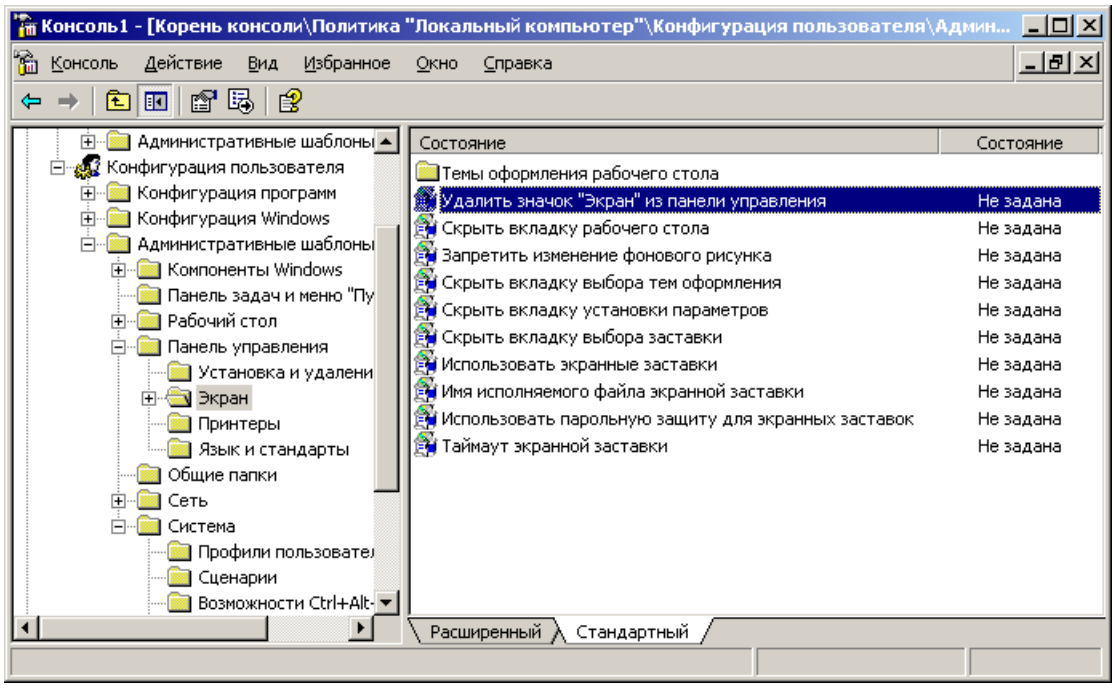


Рис. 11. Налаштування адміністративних шаблонів.

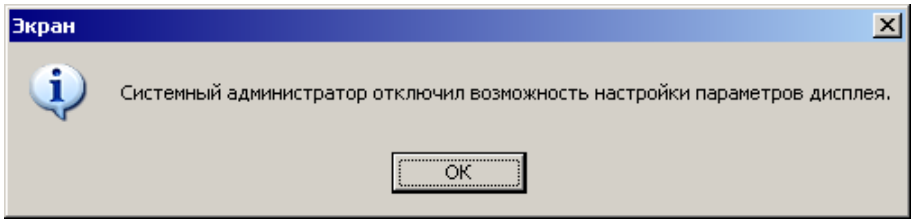


Рис. 12. Повідомлення системи щодо заборони виконання певних налаштувань робочого середовища.

5. Перейти в гілку "Политики ограниченного использования программ" (рис. 13). Створити нову політику. Не змінюючи політики за замовчуванням створити нове правило (правила), що забороняє виконання програм з будь-якого тому крім "C:" (при потребі створити логічні диски або розділи) – рис. 14, 15. Спробувати виконати будь-який файл з цього тому (рис. 16). Створити нове правило для хешу програми, яке дозволить виконувати саме цей вказаний файл (рис. 17). Спробувати запустити на виконання цей файл. Для яких потреб можуть використовуватись правила такого типу?

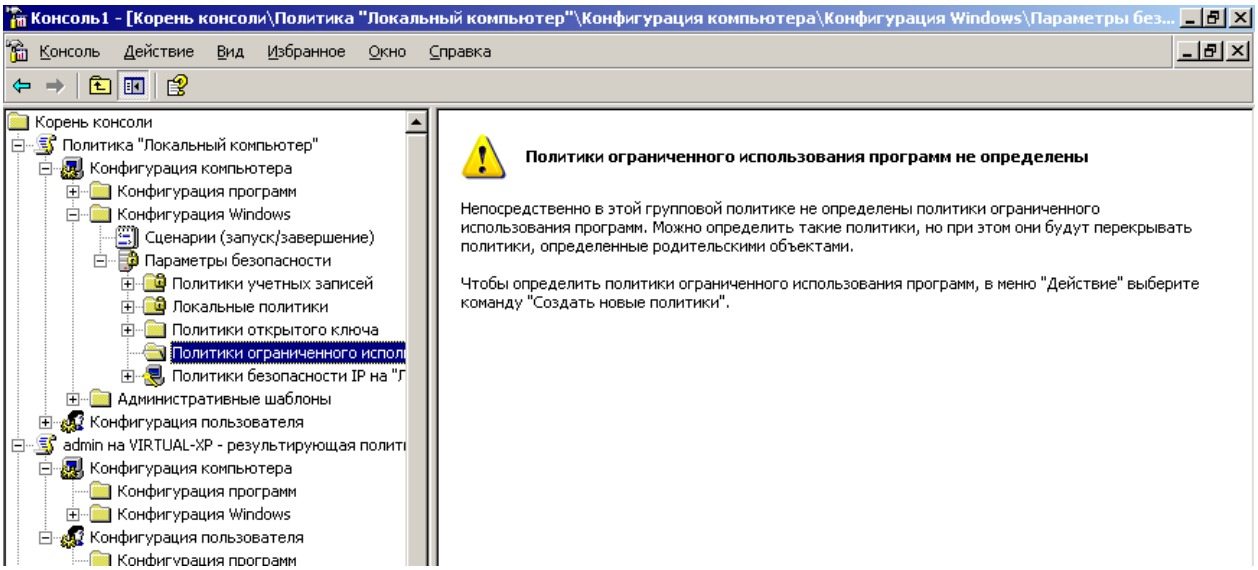


Рис. 13. Загальний вигляд гілки обмеженого використання програм.

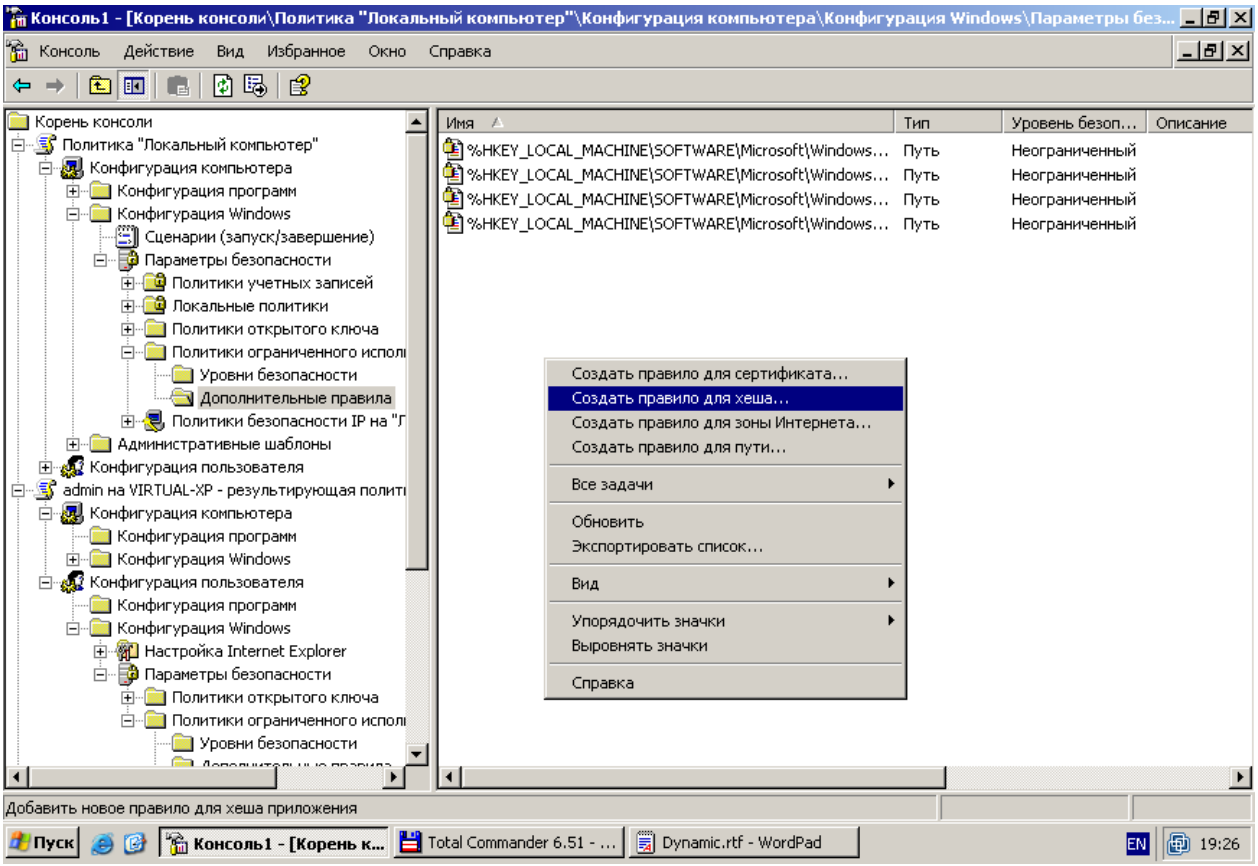


Рис. 14. Створення правил обмеженого використання програм.

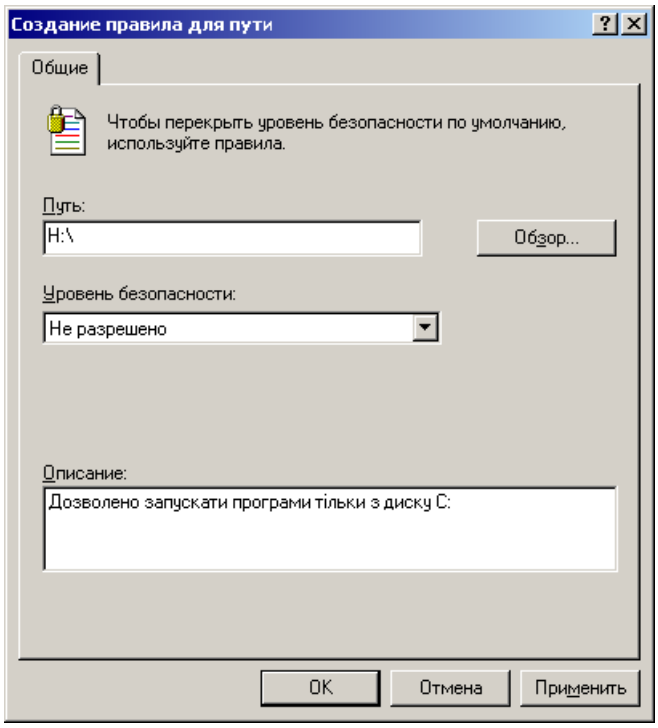


Рис. 15. Властивості правила обмеженого використання програм.

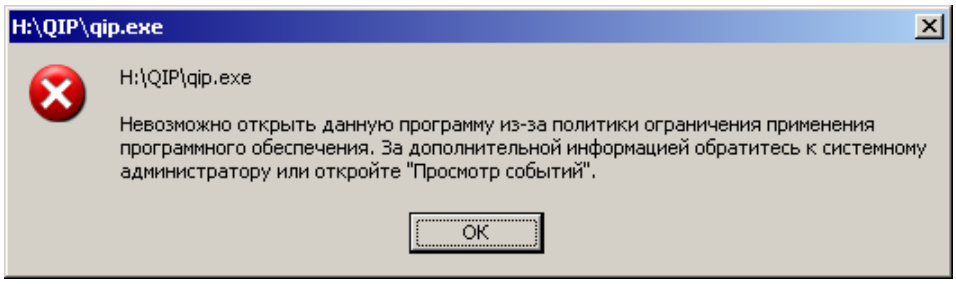


Рис. 16. Повідомлення системи про заборону виконання програми.

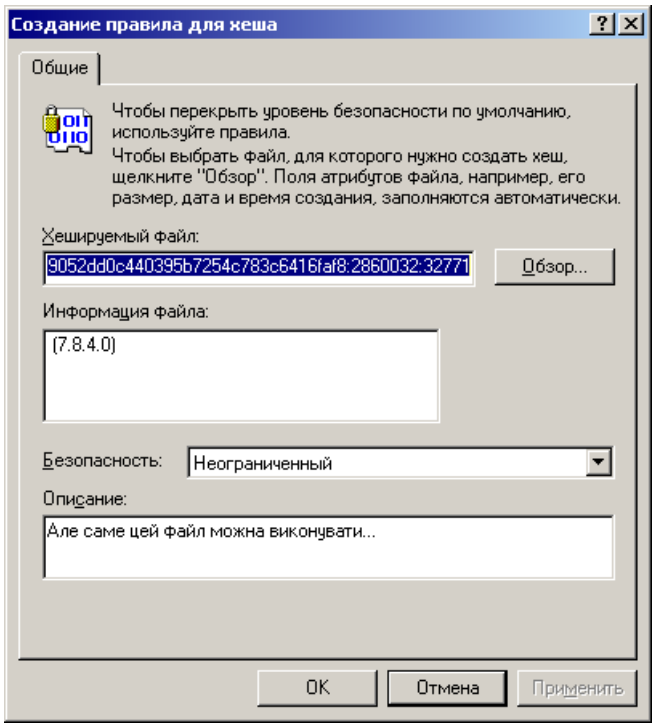


Рис. 17. Створення правила для хеша.

6. Відкрити оснастку mmc "Анализ и настройка безопасности" (рис. 18). Створити нову базу даних, яка буде відображати стан налаштування політик комп'ютера за певним шаблоном.

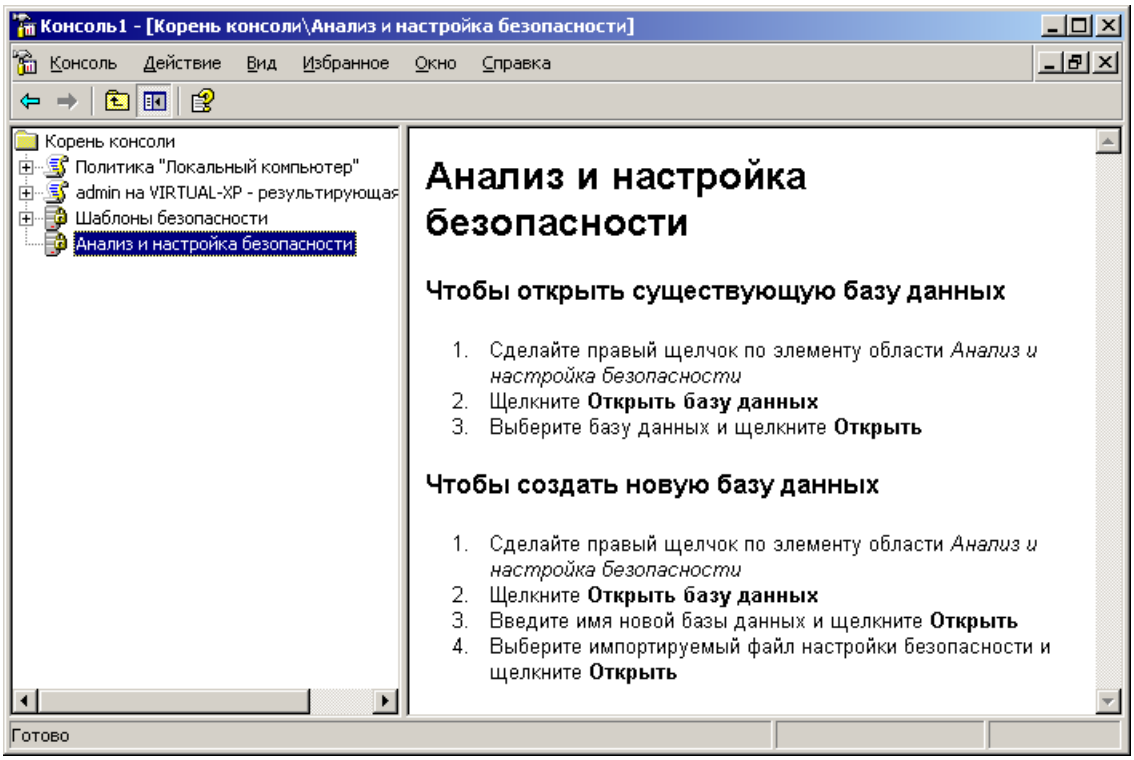


Рис. 18. Оснащення "Аналіз і налаштування безпеки".

Для порівняння обрати один із вбудованих шаблонів безпеки – рис. 19 (власні шаблони можна створювати за допомогою оснастки "Шаблоны безопасности"). Проаналізувати параметри безпеки комп'ютера (рис. 20). Результати аналізу відображаються як порівняння параметрів комп'ютера з параметрами шаблону (створеної бази даних) – рис. 21. Базу даних можна редагувати в цьому ж вікні, а потім вибрати пункт контекстного меню "Сохранить" та, при потребі, експортувати відредагований шаблон безпеки.

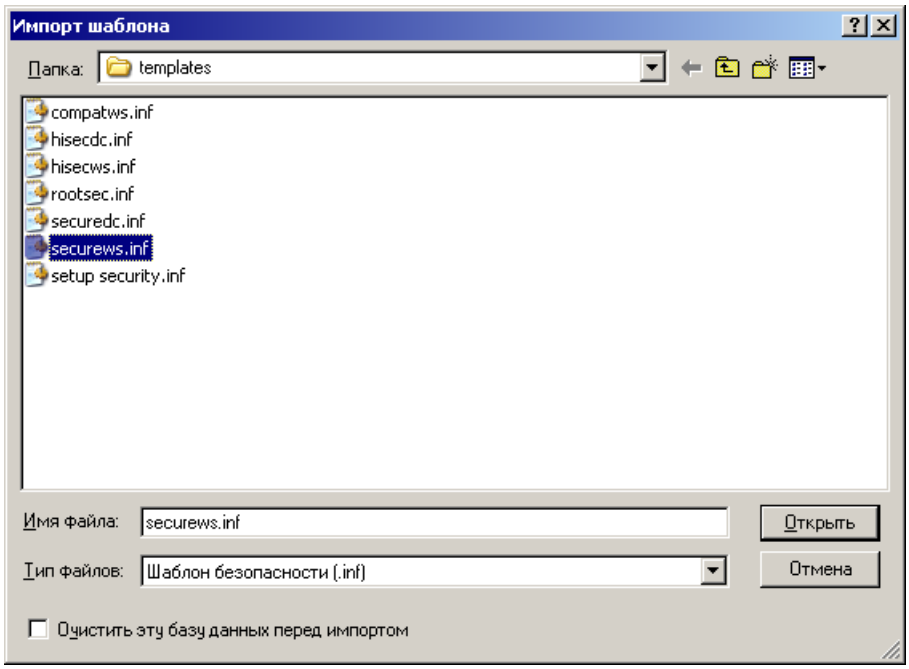


Рис. 19. Імпорт шаблону безпеки з файлу.

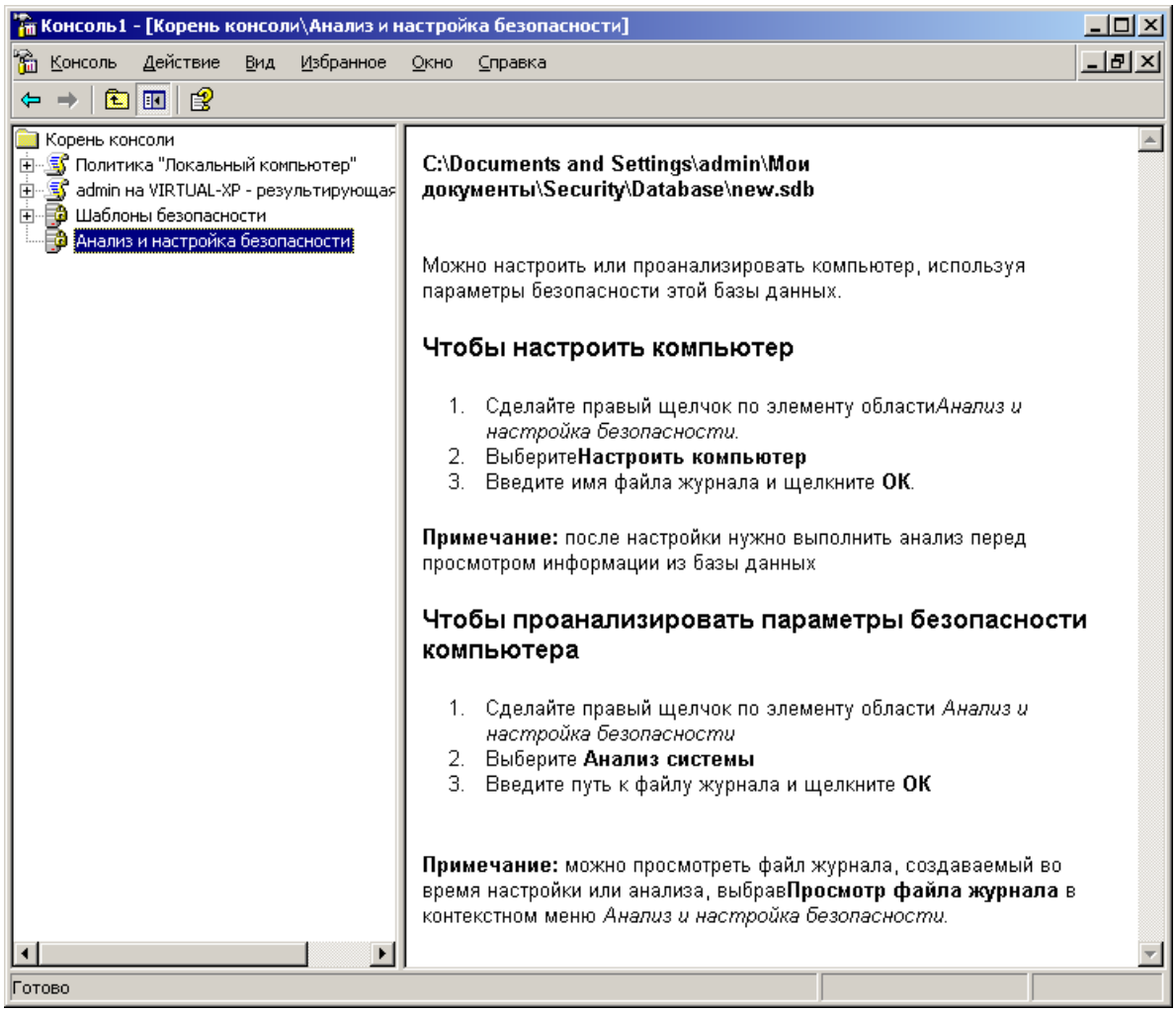


Рис. 20. Використання оснащення "Аналіз і налаштування безпеки".

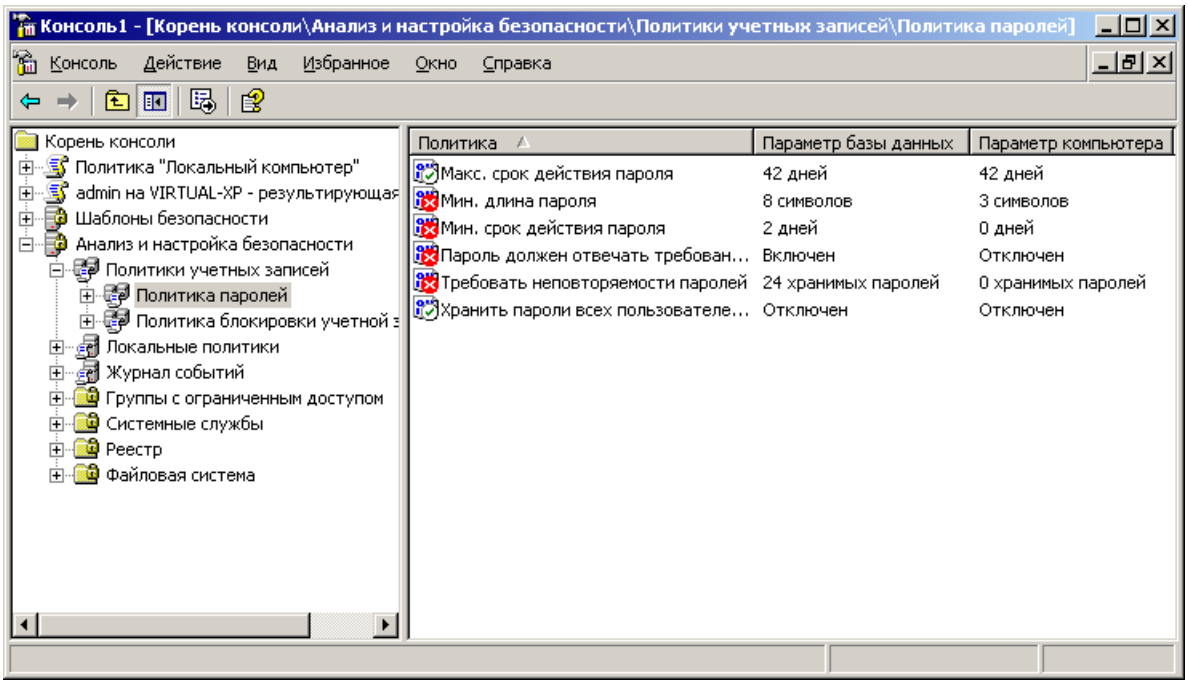


Рис. 21. Результат аналізу безпеки системи.

Налаштувати комп’ютер за певним шаблоном безпеки (привести у відповідність параметри бази даних і поточні налаштування комп’ютера), виконавши необхідні дії (рис. 20).

У звіті до лабораторної роботи описати та пояснити отримані результати.

Контрольні запитання.

1. Призначення групових політик.
2. Чим відрізняються гілки політики "Конфигурация компьютера" та "Конфигурация пользователя"?
3. Хто має привілей брати об’єкти у власність?
4. Порядок застосування групових політик в Active Directory.
5. Для чого використовуються шаблони безпеки?
6. Чи можна (і як) за допомогою політик бути впевненим у відсутності модифікацій програмного забезпечення після його встановлення на комп’ютер?

Лабораторна робота № 2.
АУДИТ. ПОЛІТИКИ АУДИТУ. РОБОТА З ЖУРНАЛОМ БЕЗПЕКИ WINDOWS.

Мета роботи: Ознайомлення з політиками та налаштуванням аудиту, аналізом безпеки системи шляхом вивчення журналу подій в Windows XP. Навчитись проводити аудит локальної системи та працювати з журналом безпеки Windows.

Теоретичні відомості.

Аудит дозволяє відстежувати і записувати події, пов'язані з безпекою, такі, як спроби доступу користувачів до захищених файлів і папок. Після включення аудиту об'єкту в журнал безпеки Windows XP Professional заносяться записи при будь-якій спробі доступу до цього об'єкту. При цьому визначається об'єкт аудиту, дії, що піддаються аудиту, і точні типи дій для аудиту. Після установки аудиту можна відстежувати доступ користувачів до певних об'єктів і аналізувати недоліки системи безпеки. Записи аудиту, що містять відомості по вибраним подіям, показують, хто виконував певні дії і хто намагався виконати певні недозволені дії.

Найбільш загальними типами подій для аудиту є:

- доступ до таких об'єктів, як файли і папки;
- управління обліковими записами користувачів і груп;
- вхід користувачів в систему і вихід з неї.

Політики аудиту. Перед впровадженням аудиту необхідно вибрати політику аудиту. Політика вказує категорії подій аудиту, пов'язаних з безпекою. При першій установці Windows XP Professional усі категорії аудиту вимкнені. Включаючи аудит різних категорій подій, можна створювати політику аудиту, що задовольняє всім вимогам організації.

Для проведення аудиту можна вибрати наступні категорії подій:

- Аудит подій входу в систему;
- Аудит управління обліковими записами;
- Аудит доступу до служби каталогів;
- Аудит входу в систему;
- Аудит доступу до об'єктів;
- Аудит зміни політики;
- Аудит використання привілеїв;

- Аудит відстеження процесів;
- Аудит системних подій.

Якщо як частина політики аудиту вибраний аудит доступу до об'єктів, необхідно включити або категорію аудиту доступу до служби каталогів (для аудиту об'єктів на контролері домену), або категорію аудиту доступу до об'єктів (для аудиту об'єктів на рядовий сервер або робочу станцію). Після включення категорії доступу до об'єктів можна вказати для кожної групи або користувача, для яких типів доступу проводити аудит.

Щоб включити аудит локальних об'єктів, необхідно увійти до системи з обліковим записом члена групи "Адміністратори".

У табл. 3 наведено опис категорій подій аудиту, що використовуються для створення політики.

Таблиця 3

Опис категорій аудиту

Категорія аудиту	**Опис**
Аудит подій входу в систему	Визначає, чи підлягає аудиту кожна спроба користувача увійти до системи або вийти з неї на іншому комп'ютері, за умови, що даний комп'ютер використовується для перевірки достовірності облікового запису. Якщо аудит успішних спроб входу в систему включений на контролері домену, в журнал заноситиметься запис про кожного користувача, що пройшов перевірку на цьому контролері домену, не зважаючи на те, що користувач насправді входить в систему на робочій станції домену.
Аудит управління обліковими записами	Визначає, чи підлягають аудиту всі події, пов'язані з управлінням обліковими записами на комп'ютері. До таких подій відносяться, зокрема, наступні: • створення, зміна або видалення облікового запису користувача або групи; • перейменування, відключення або включення облікового запису користувача;

	• встановлення або зміна пароля.
Аудит доступу до служби каталогів	Визначає, чи підлягає аудиту подія доступу користувача до об'єкту каталогу Active Directory, для якого задана власна системна таблиця управління доступом (SACL)[1]. Дана політика аналогічна політиці "Аудит доступу до об'єктів", тільки вона застосовується до об'єктів Active Directory, а не до об'єктів файлової системи і реєстру.
Аудит входу в систему	Визначає, чи підлягає аудиту кожна спроба користувача увійти до системи або вийти з неї на даному комп'ютері, або підключитися до нього через мережу. Якщо на контролері домену ведеться облік успішних спроб для політики "Аудит подій входу в систему", спроби входу в систему на робочих станціях не підлягатимуть аудиту. Події входу в систему реєструються тільки при спробах інтерактивного і мережного входу на сам контролер домену. Події входу в систему для облікового запису створюються на комп'ютері, де зберігається обліковий запис; події входу створюються при спробах виконати вхід.
Аудит доступу до об'єктів	Визначає, чи підлягає аудиту подія спроби доступу користувача до об'єкту (наприклад, до файлу, теки, розділу реєстру, принтера і т.д.), для якого вказаний власний список контролю системного доступу (SACL)[2].
Аудит зміни політики	Визначає, чи підлягає аудиту кожен факт зміни політик призначення прав користувачів, політик аудиту або політик довірчих відносин.
Аудит використання привілеїв	Визначає, чи підлягає аудиту кожна

[1] системну таблицю управління доступом для об'єкту Active Directory можна встановити на вкладці **Безпека** діалогового вікна **Властивості** цього об'єкту.

[2] системну таблицю управління доступом для об'єкту файлової системи можна встановити на вкладці **Безпека** діалогового вікна **Властивості** цього об'єкту.

	спроба користувача скористатися наданим йому правом. За умовчанням аудит не виконується для використання наступних прав користувача, навіть якщо заданий аудит успіхів і відмов для параметра "Аудит використання привілеїв". • Обхід перехресної перевірки; • Відлагодження програм; • Створення маркерного об'єкту; • Заміна маркера рівня процесу; • Створення журналів безпеки; • Архівація файлів і каталогів; • Відновлення файлів і каталогів.
Аудит відстеження процесів	Визначає, чи підлягають аудиту такі події, як активізація програми, завершення процесу, повторення дескрипторів і непрямий доступ до об'єкту.
Аудит системних подій	Визначає, чи підлягають аудиту події перевантаження або вимкнення комп'ютера, а також події, що впливають на системну безпеку або на журнал безпеки.

У табл. 4 представлені різні події аудиту і ті загрози безпеці, які відображаються за допомогою цієї події.

Таблиця 4

Потенційні загрози безпеці, що можуть бути виявлені за допомогою аудиту

Подія аудиту	**Потенційна загроза**
Аудит відмов входу/виходу.	Випадковий злом пароля
Аудит успіхів входу/виходу.	Вхід з вкраденим паролем
Аудит успіхів використання привілеїв, управління користувачами і групами, змін політик безпеки, перевантаження, вимкнення і системних подій.	Неправильне використання привілеїв
Аудит успіхів і відмов подій доступу до файлів і об'єктів. Аудит успіхів і відмов диспетчера файлів в доступі підозрілим	Неправильний доступ до

користувачам або групам до важливих файлів для читання і запису.	важливих файлів
Аудит успіхів і відмов подій доступу до принтерів і об'єктів. Аудит успіхів і відмов диспетчера друку в доступі підозрілим користувачам або групам до принтерів.	Неправильний доступ до принтерів
Аудит успіхів і відмов доступу для запису до програмних файлів (з розширеннями .exe і .dll). Аудит успіхів і відмов для відстеження процесів. Запустіть підозрювану програму; перевірте наявність в журналі безпеки неприпустимих спроб змінити програмні файли або створити невірні процеси. Запускайте програму, тільки відстежуючи події в журналі системи.	Епідемія вірусів

Налаштування аудиту може виконуватися як в один, так і в два прийоми:

1. Спочатку його слід активізувати за допомогою оснащення **Local Security Settings** (Локальна політика безпеки) або **Group Policy Object Editor** (Редактор об'єктів групової політики). При цьому необхідно визначити набір (тип) категорій подій. Для більшості категорій подій (крім аудиту доступу до об'єктів та аудиту доступу до служби каталогів) цієї операції достатньо, і їх реєстрація починається негайно.
2. Потім слід вказати, які конкретно об'єкти необхідно піддати аудиту, і для яких груп або користувачів він здійснюватиметься. Ця операція виконується за допомогою Редактора списків управління доступом (ACL) на вкладці **Безпека** діалогового вікна **Властивості** відповідного об'єкту[1].

Перегляд системних подій. В операційних системах Windows подією називається будь-який значний "випадок" в роботі системи або додатку, про який слід повідомити користувачів. У разі виникнення критичних подій, таких як переповнення диска сервера або неполадки з електроживленням, на екран монітора буде виведено відповідне повідомлення. Решта подій, які не вимагають негайних дій від користувача, реєструється в системних журналах. Служба реєстрації подій в системних журналах активується автоматично при кожному запуску системи Windows XP.

Оснащення Event Viewer. У системі Windows Server 2003 для перегляду системних журналів можна використовувати оснащення **Event Viewer** (Перегляд подій). Це оснащення можна також запустити з вікна оснащення

[1] Нагадаємо, що аудит можливий тільки на томах NTFS.

Computer Management (Управління комп'ютером). На рис. 22 показаний приклад вікна оснащення **Event Viewer**.

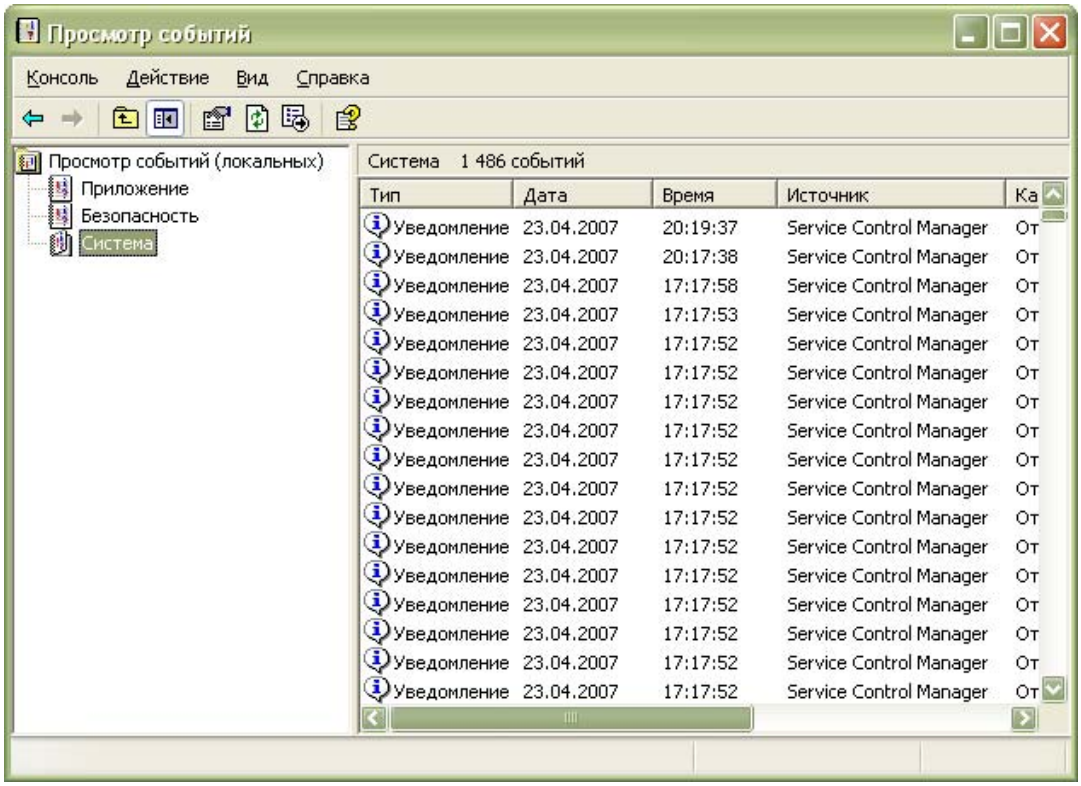


Рис. 22. Вікно оснащення Event Viewer.

За допомогою оснащення **Event Viewer** можна проглядати три типи стандартних (основних) журналів[1].

- Журнал додатків (Application log) – фіксує події, зареєстровані додатками. Наприклад, текстовий редактор може зареєструвати в даному журналі помилку при відкритті файлу.
- Журнал системи (System log) – записує події, які реєструються системними компонентами Windows. Наприклад, в системний журнал записуються такі події, як збій в процесі завантаження драйвера або іншого системного компоненту при запуску системи.
- Журнал безпеки (Security log) – містить записи, пов'язані з системою безпеки. За допомогою цього журналу можна відстежувати зміни в системі безпеки і ідентифікувати діри в захисті. У даному журналі можна реєструвати спроби входу в систему. Для перегляду журналу

[1] Крім стандартних, на комп'ютері – в першу чергу на контролері домену – можуть бути і інші журнали, створювані різними службами (наприклад, Active Directory, DNS, File Replication Service і т. д.). Робота з такими журналами нічим не відрізняється від процедур перегляду стандартних журналів.

необхідно мати права адміністратора. За умовчанням реєстрація подій в журналі безпеки відключена.

Типи подій. Нижче перераховані типи подій, що реєструються в журналах.

- **Error** (Помилка) – подія реєструється у разі виникнення серйозної події (такої як втрата даних або функціональних можливостей). Подія даного типу буде зареєстрована, якщо неможливо завантажити яку-небудь з служб в ході запуску системи.
- **Warning** (Попередження) – подія не є серйозною, але може привести до виникнення проблем в майбутньому. Наприклад, якщо недостатньо дискового простору, то буде зареєстровано попередження.
- **Information** (Повідомлення) – значуща подія, яка свідчить про успішне завершення операції додатком, драйвером або службою. Таку подію може, наприклад, зареєструвати мережний драйвер, що успішно завантажився.
- **Success Audit** (Аудит успіхів) – подія, пов'язана з безпекою системи. Прикладом такої події є успішна спроба реєстрації користувача в системі.
- **Failure Audit** (Аудит відмов) – подія пов'язана з безпекою системи. Наприклад, така подія буде зареєстрована, якщо спроба доступу користувача до мережного диску закінчилася невдачею.

Параметри подій. Інформація про події містить наступні параметри:

- **Type** (Тип) – тип події;
- **Date** (Дата) – дата генерації події;
- **Time** (Час) – час реєстрації події;
- **Source** (Джерело) – джерело (ім'я програми, системного компоненту або компоненту додатку), яке привело до реєстрації події;
- **Category** (Категорія) – класифікація події по джерелу, що викликало її появу;
- **Event ID** (Подія) – ідентифікатор події;
- **User** (Користувач) – обліковий запис користувача, від імені якого проводилися дії, що викликали генерацію події;
- **Computer** (Комп'ютер) – комп'ютер, на якому зареєстровано подію.

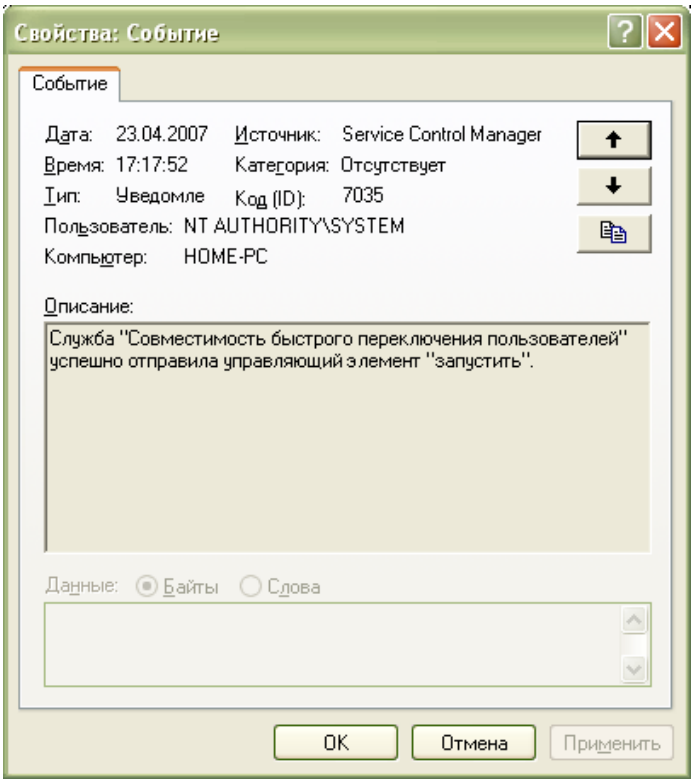


Рис. 23. Додаткова інформація про подію.

Для перегляду додаткової інформації про подію виберіть в меню **Action** (Дія) пункт **Properties** (Властивості) (або клацніть двічі кнопкою миші на рядку в списку подій). З'явиться вікно, приклад якого показаний на рис. 23. На панелі **Description** (Опис) приведена загальна інформація про подію. На панелі **Data** (Дані) відображаються двійкові дані, які можуть бути представлені як **Bytes** (Байти) або як **Words** (Слова). Ці дані можуть бути інтерпретовані досвідченим програмістом або технічним фахівцем служби підтримки, знайомим з вихідним кодом додатку.

Завдання до виконання роботи

1. Відкрити оснастку mmc "Групповая политика". Перейти в гілку "Политика аудита" (рис. 24), включити аудит доступу до об’єктів (рис. 25). Після цього у властивостях безпеки об’єкту, за яким повинно проводитись спостереження (папки чи файлу), перейти у вкладку "Аудит" (рис. 26а) та увімкнути аудит для визначених суб’єктів безпеки та їх активності (наприклад видалення – рис. 26б). (Переконатись, що без налаштування аудиту на об’єкті файлової системи записів в журнал не відбувається – п. 2.) Виконати умови аудиту (тобто дії над цим об’єктом та тим користувачем для яких налаштовано аудит).

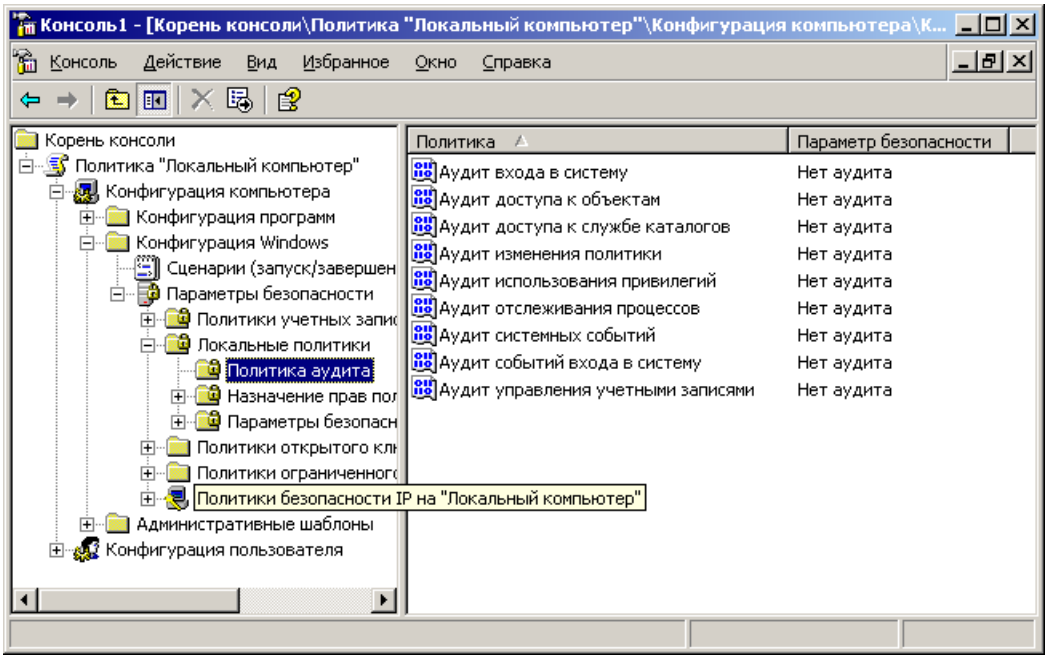


Рис. 24. Гілка політики аудиту в об’єкті групової політики.

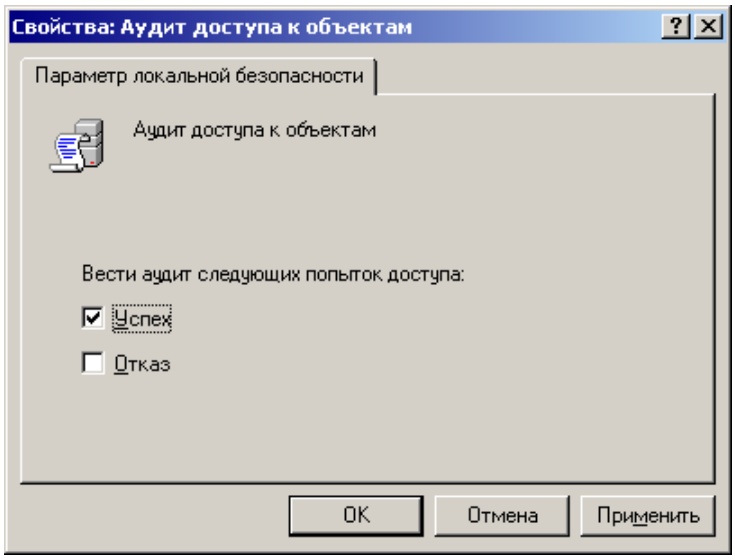
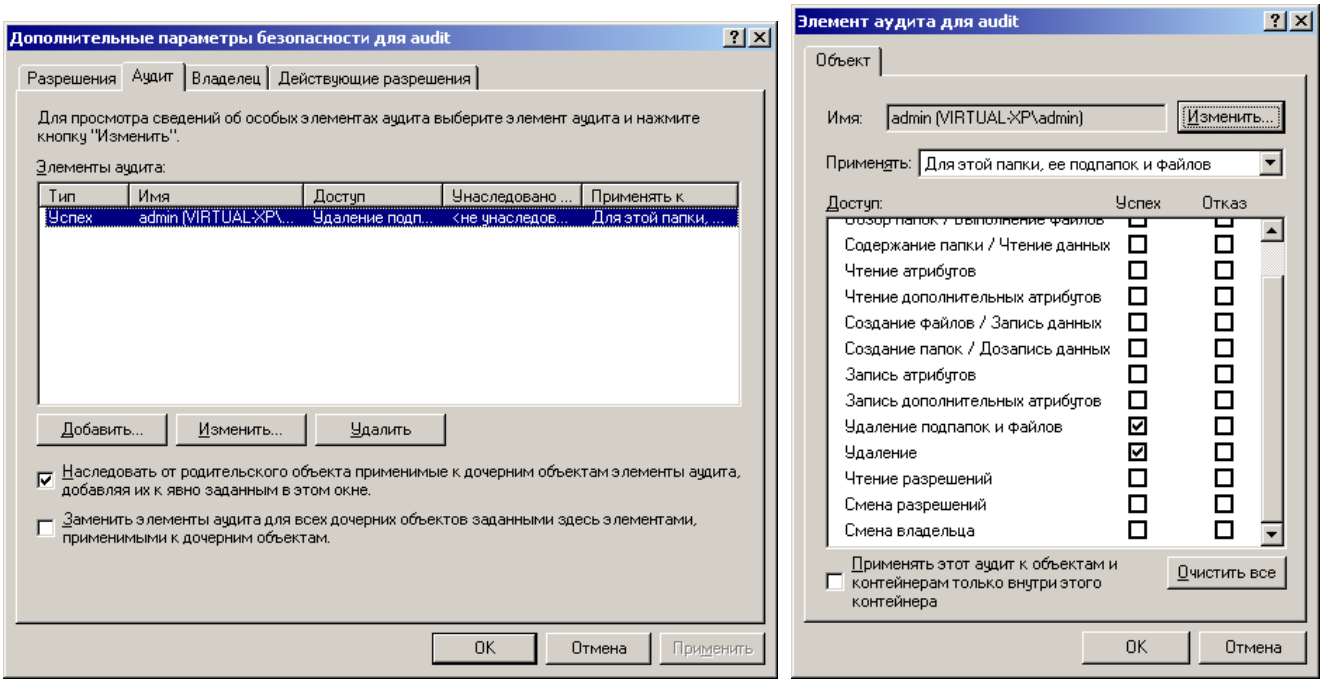


Рис. 25. Включення політики аудиту.



3 б

Рис. 26. Налаштування аудиту доступу до об’єктів на об’єктах файлової системи.

2. Відкрити оснастку mmc "Просмотр событий" та журнал "Безопасность" в ній (рис. 27). Знайти в журналі записи категорії "Доступ к объектам" та записи про дію, яку контролювалося (рис. 28). (Додаткові відомості про подію за номером її коду (ID) можна знайти на сайті Microsoft або в Resource Kit).

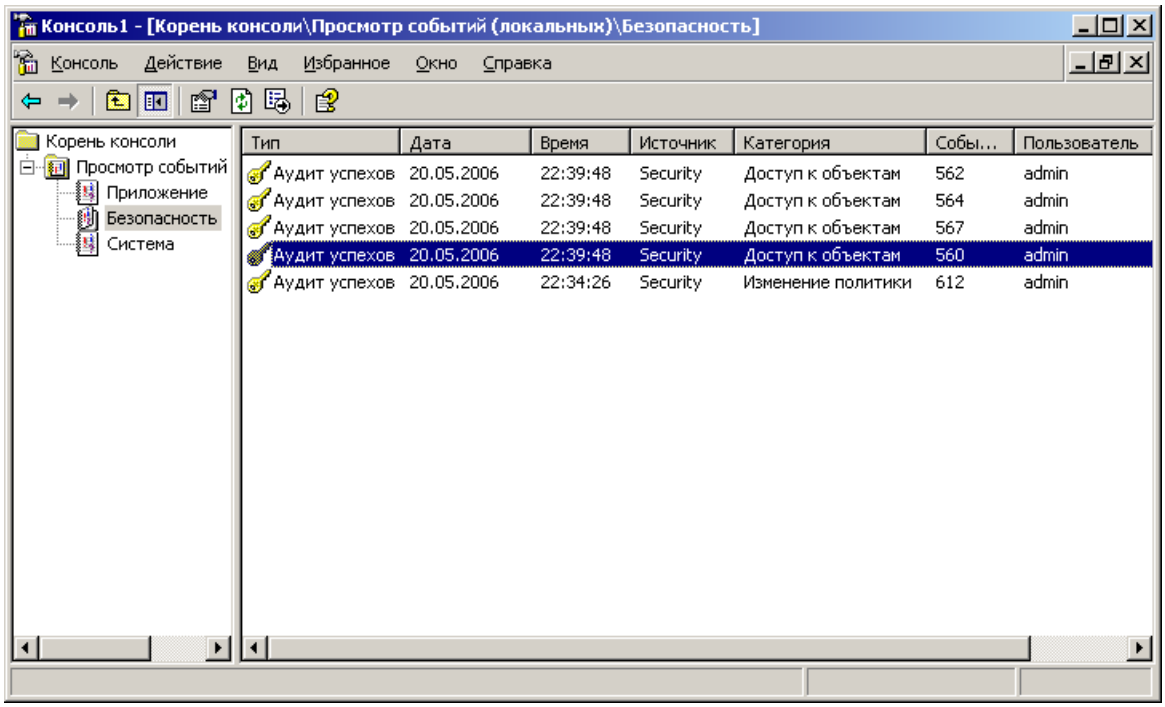
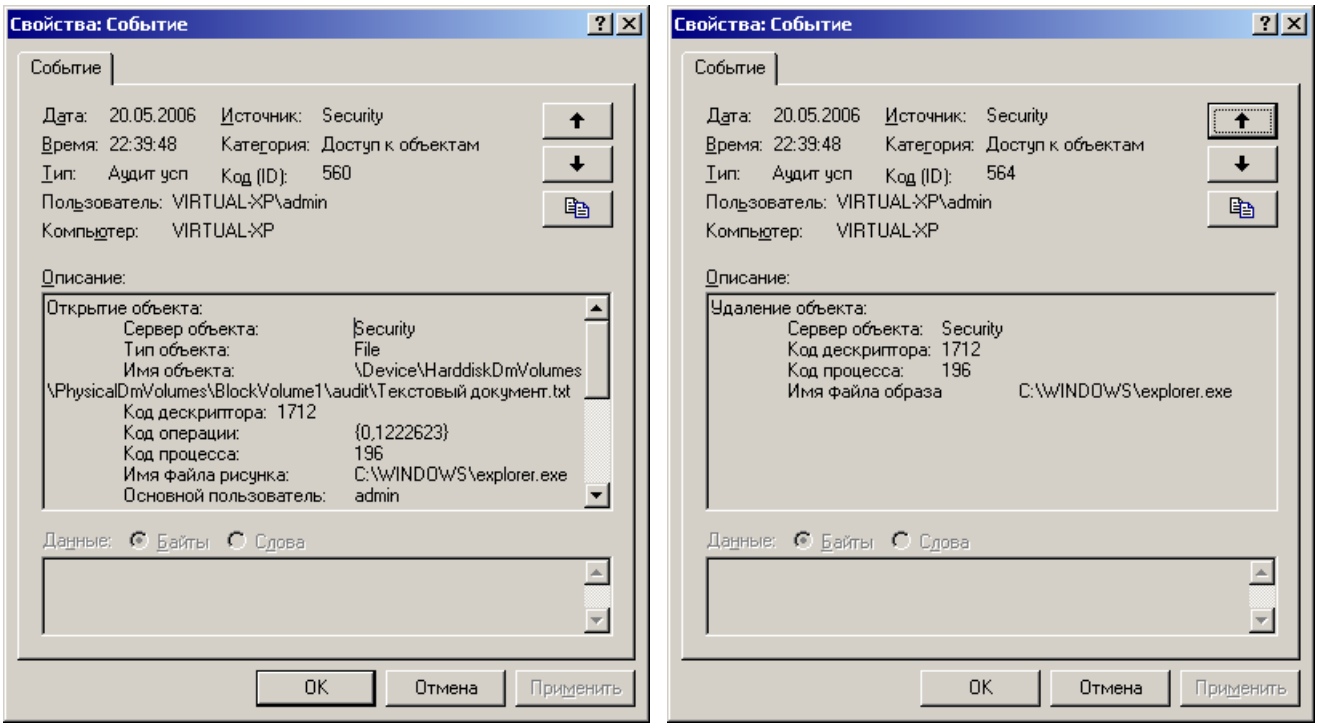


Рис. 27. Записи про події аудиту в журналі безпеки.

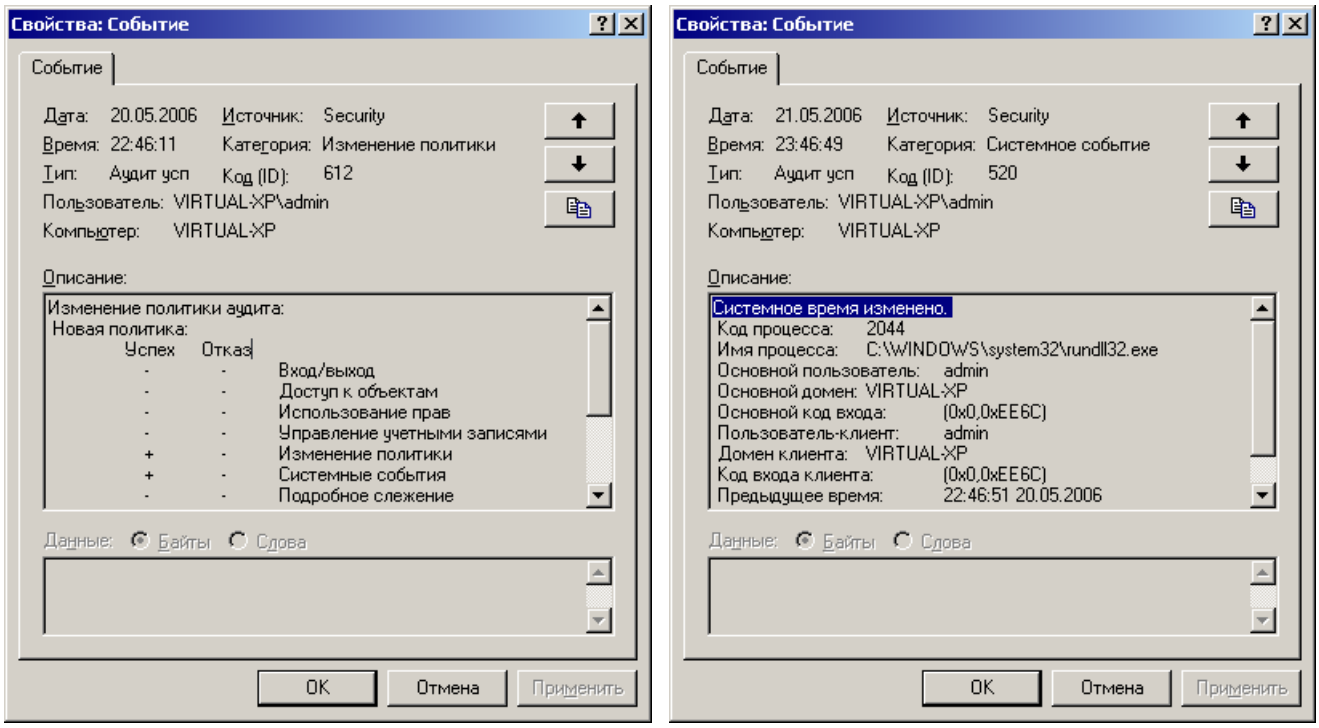


а б

Рис. 28. Детальний опис запису в журналі безпеки.

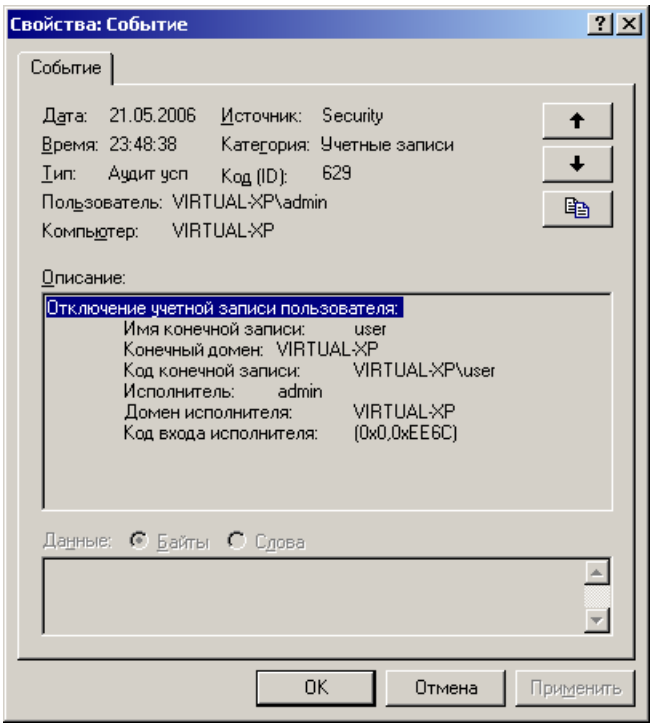
3. В політиках аудиту увімкнути аудит зміни політики та системних подій. Виконати умови аудиту (наприклад змінити системний час). В журналі безпеки відстежити записи про ці події (рис. 29). Увімкнути аудит управління обліковими записами користувачів; відключити обліковий запис існуючого

користувача, створити нового користувача, задати пароль користувачу. В журналі безпеки відстежити записи про ці події (рис. 30). Увімкнути аудит входу в систему; вийти зі системи та зайти під іншим користувачем. В журналі безпеки знайти записи категорії "Вход/Выход" (рис. 31) та відстежити записи про ці події (рис. 32).

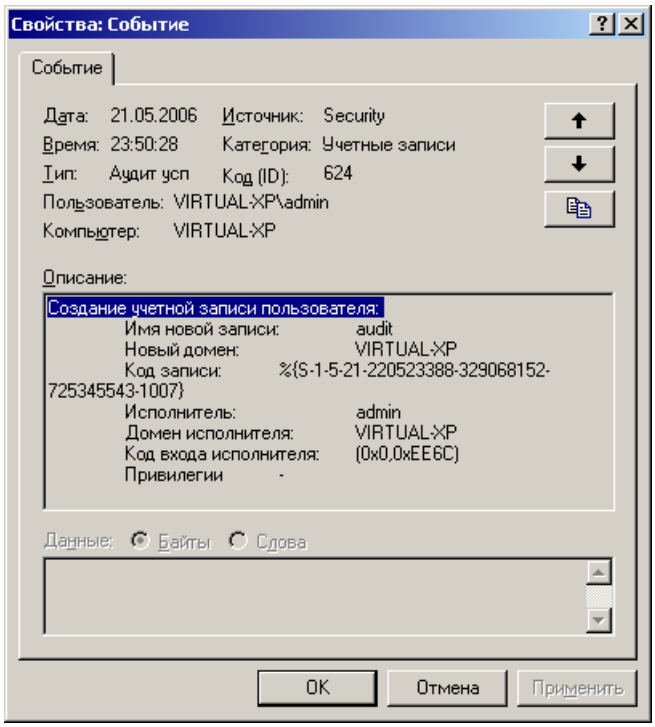


з б

Рис. 29. Записи подій різних політик аудиту.



а



б

Рис. 30. Записи подій аудиту управління обліковими записами.

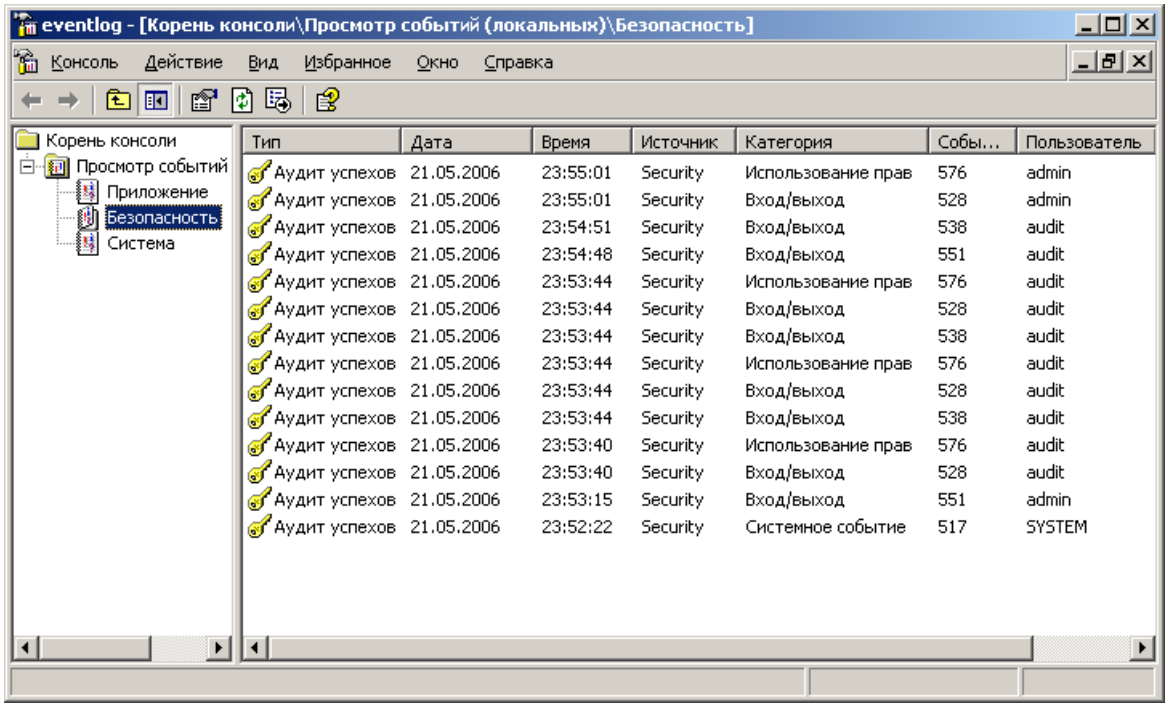
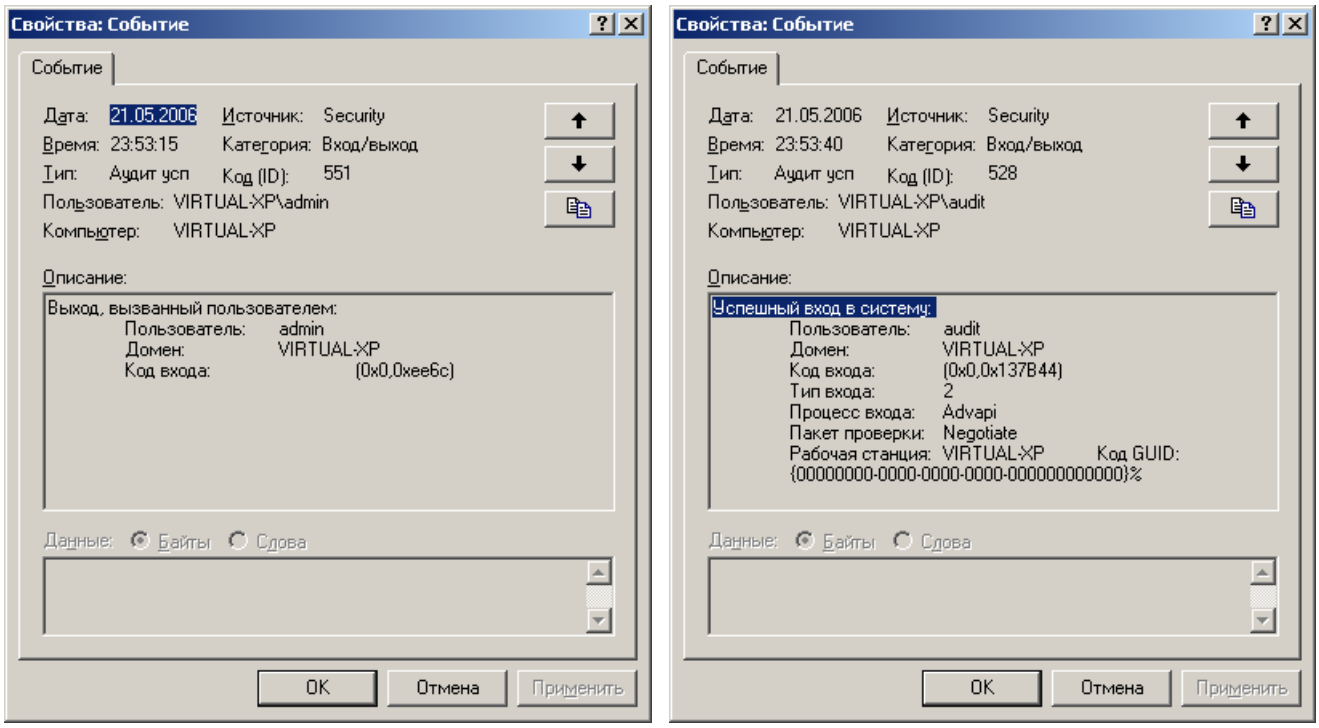


Рис. 31. Журнал безпеки системи.



а б

Рис. 32. Відомості про вхід та вихід користувача з системи.

4. В контекстному меню журналу безпеки вибрати пункт "Свойства" (рис. 33). Задати якнайменший розмір журналу та політику "Не затирать события". Після цього в редакторі об’єкту групової політики (гілка "Параметры безопасности") включити параметр політики "Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности" (рис. 34). Заповнити журнал аудиту увімкнувши політики та виконавши достатню кількість дій, що підлягають аудиту. Якщо це виконувалось користувачем з адміністративними повноваженнями, спробувати увійти в систему як звичайний користувач. Переконатись у неможливості входу в систему через переповненість журналу аудиту (рис. 35). Увійти як адміністратор; вимкнути увесь аудит. В контекстному меню журналу безпеки вибрати пункт "Стереть все события" для очищення журналу. Чи усі події вдалося видалити? Чи з’явились нові записи?

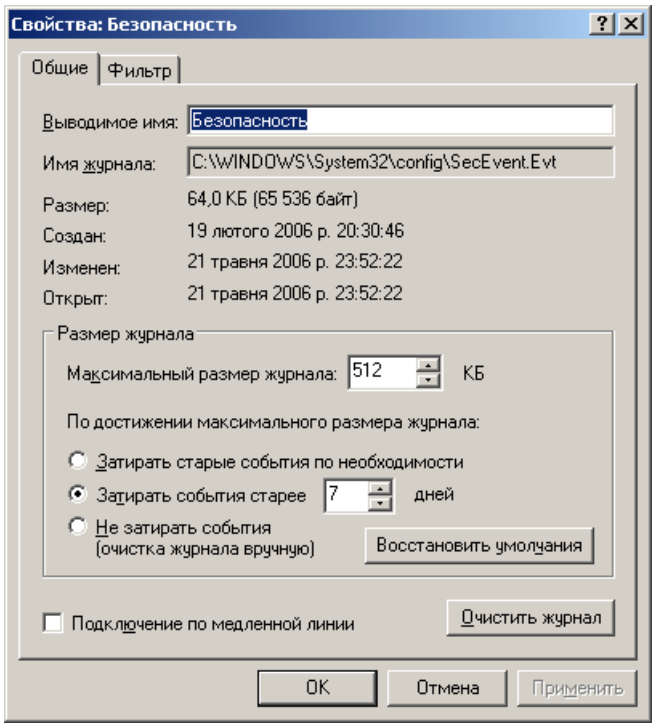


Рис. 33. Налаштування журналу безпеки Windows.

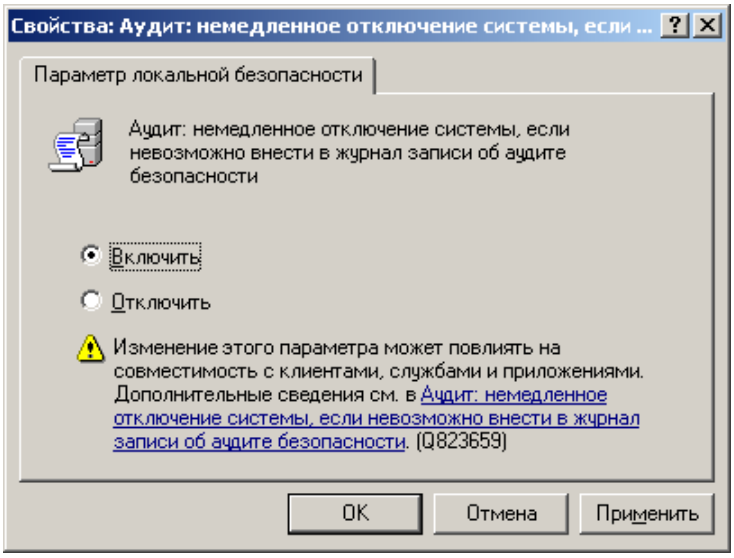


Рис. 34. Налаштування параметру безпеки для заборони входу в систему при переповненні журналу безпеки.

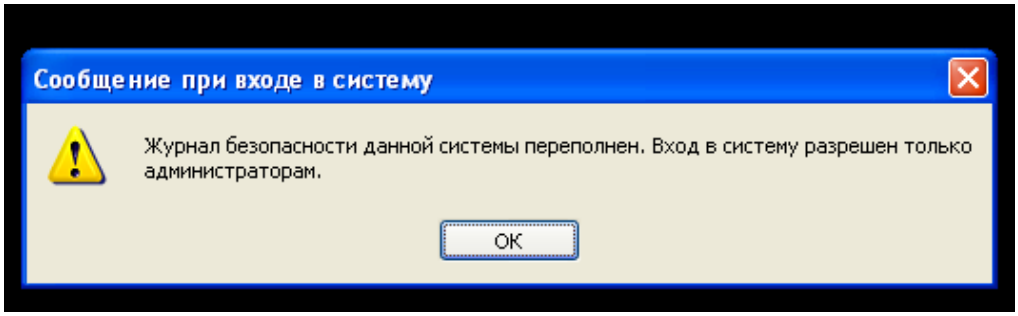


Рис. 35. Системне повідомленя про переповнення журналу безпеки.

У звіті до лабораторної роботи описати та пояснити отримані результати.

Контрольні запитання.

1. Що таке аудит?
2. Які існують політики аудиту в Windows?
3. Включення якої політики аудиту не приводить до автоматичної появи записів в журналі?
4. Які записи аудиту з’являються в журналі автоматично, навіть без включення відповідної політики?
5. Як називається та яким оснащенням можна переглянути журнал аудиту в Windows?
6. Який мінімальний розмір журналу аудиту в Windows XP?

СПИСОК ЛІТЕРАТУРИ

1. **Microsoft Corporation** Microsoft Windows XP Professional. Учебный курс MCSA/MCSE. – М.: Издательско-торговый дом "Русская Редакция", 2003. – 1008 стр.
2. **Microsoft Corporation** Microsoft Windows 2000 Active Directory Services. Учебный курс MCSE. – М.: Издательско-торговый дом «Русская редакция», 2004. – 608 с.
3. **Руссинович М.**, **Соломон Д.** Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. – М.: Издательско-торговый дом «Русская редакция»; СПб.: Питер, 2005. – 992 с.
4. **Вишневский А**. Windows Server 2003. Для профессионалов. – СПб.: Питер, 2004. – 767 с.
5. **К. Айвенс** Microsoft Windows Server 2003. Полное руководство. – М.: Издательство "СП ЭКОМ", 2004.– 896 с.

НАВЧАЛЬНЕ ВИДАННЯ

АУДИТ І НАЛАШТУВАННЯ БЕЗПЕКИ У WINDOWS XP

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторних робіт
з дисципліни „Адміністрування та безпека комп'ютерів"
для студентів спеціальності
„Програмне забезпечення автоматизованих систем"

Укладачі Яковина Віталій Степанович
Білас Орест Євгенович

Редактор

Комп'ютерне верстання