Товариство з обмеженою відповідальністю
Науково-дослідний інститут
«Автопром»

Система захисту інформації

ЛОЗА™-1

версія 4.4.0

ПРОГРАМНІ ЗАСОБИ АДМІНІСТРУВАННЯ СИСТЕМИ

ІНСТРУКЦІЯ КОРИСТУВАЧА

ЛОЗА-1-4.І3.06.1

ТОВ НДІ “Автопром”
Київ, 2020

Зміст

Вступ

Документ містить інструкції з експлуатації програмних засобів, призначених для адміністрування системи ЛОЗА-1. Він призначений для використання системним адміністратором та адміністратором безпеки.

Будову та порядок функціонування системи докладно описано в документі “Загальний опис системи”. Відомості, викладені в цьому документі, використовуються далі без посилання на нього.

1 Загальні положення

Для роботи адміністраторів системи розроблено такі програмні засоби:

– програма ***Аудитор***, яка дозволяє переглядати журнал реєстрації подій, створювати його резервні копії та формувати й друкувати протоколи роботи системи;

– програма ***Керування захистом***, призначена для вирішення завдань, пов'язаних із керуванням доступом, та визначення параметрів конфігурації системи;

– програма ***Монітор захисту***, призначена для оперативного керування системою та спостереження за її роботою.

Для роботи системи необхідні нижченаведені програмні засоби:

– операційна система MS Windows 7/8.1/10/2012/2016/2019;

– Microsoft Word та Microsoft Excel із набору MS Office версії 2007/2010/2013/2016/2019.

2 Програма *Аудитор*

2.1 Призначення та основні функції

Програму *Аудитор* призначено для роботи з *журналом реєстрації подій*. Цей журнал формується із подій аудиту, які реєструються системою ЛОЗА-1 та подіями, імпортованими з журналів Windows, відповідно до значень параметрів конфігурації `перелік подій, які імпортуються до журналу реєстрації` та `імпортувати всі помилки` (тут і далі `рівномірним шрифтом` виділено параметри конфігурації). Журнал реєстрації має структуру, аналогічну структурі журналів Windows.

Програма *Аудитор* дозволяє також працювати із резервними копіями журналу реєстрації.

Програма *Аудитор* надає такі можливості:
- перегляд журналу реєстрації;
- створення резервних копій журналу реєстрації та робота з ними;
- формування та друк звіту та протоколів.

2.2 Робота із програмою

У таблиці 2.1 наведено опис головного меню програми.

Таблиця 2.1 – Опис головного меню програми *Аудитор*

Меню	Підменю	Кнопка	Дія
Журнал	Журнал реєстрації подій		Відкрити журнал реєстрації подій системи "Лоза"
	Відкрити		Відкрити файл резервної копії журналу
	Додати файл журналу		Додати файл журналу до поточного перегляду
	Зберегти як		Зберегти файл журналу поточного перегляду як резервну копію
	Очистити		Очистити журнал реєстрації подій системи "Лоза"
	Вихід Alt+F4		Закінчити роботу з програмою
Вигляд	Усі події		Відмінити раніше встановлену фільтрацію подій
	Фільтр		Встановити умови відбору подій
	Пошук Ctrl+F		Почати пошук подій за встановленими критеріями
	Пошук далі F3		Продовжити пошук за встановленими раніше критеріями

Меню	Підменю	Кнопка	Дія
	Відомості… Enter		Переглянути відомості про подію
	Поновити F5		Поновити дані в журналі (з урахуванням подій, які відбулися після того, як журнал було відкрито для перегляду)
	Колонки		Налаштування колонок для перегляду журналу
	Опис події		Режим функціонує як перемикач для відображення або не відображення у головному вікні програми опису поточної події
Протоколи	Звіт про помилки та небезпечні події		Сформувати звіт про помилки та небезпечні події (тільки для поточного журналу реєстрації подій системи "Лоза")
	Протокол друку		Сформувати протокол друку документів
	Протокол за вибором		Сформувати протокол подій за вибором (встановленою умовою, у т.ч. усіх подій)
Налашту-вання	Шрифт		Вибрати шрифт для перегляду журналу
	Виділяти небезпечні події		Виділяти або ні при перегляді кольором небезпечні події
Допомога	Зміст F1		Переглянути файл інтерактивної довідки
	Про програму		Переглянути загальну інформацію про програму (версію, розробника і т.п.)

2.2.1 Перегляд журналу реєстрації

2.2.1.1 Перегляд та сортування подій

Кожний рядок журналу відповідає одній події і складається із заголовка та опису події. Заголовок події відображається на екрані і складається з таких атрибутів події:

тип;
дата та час;
джерело;
категорія;
код події;
ім’я користувача;
ім’я комп’ютера.

Далі наведено головне вікно програми (рисунок 2.1).

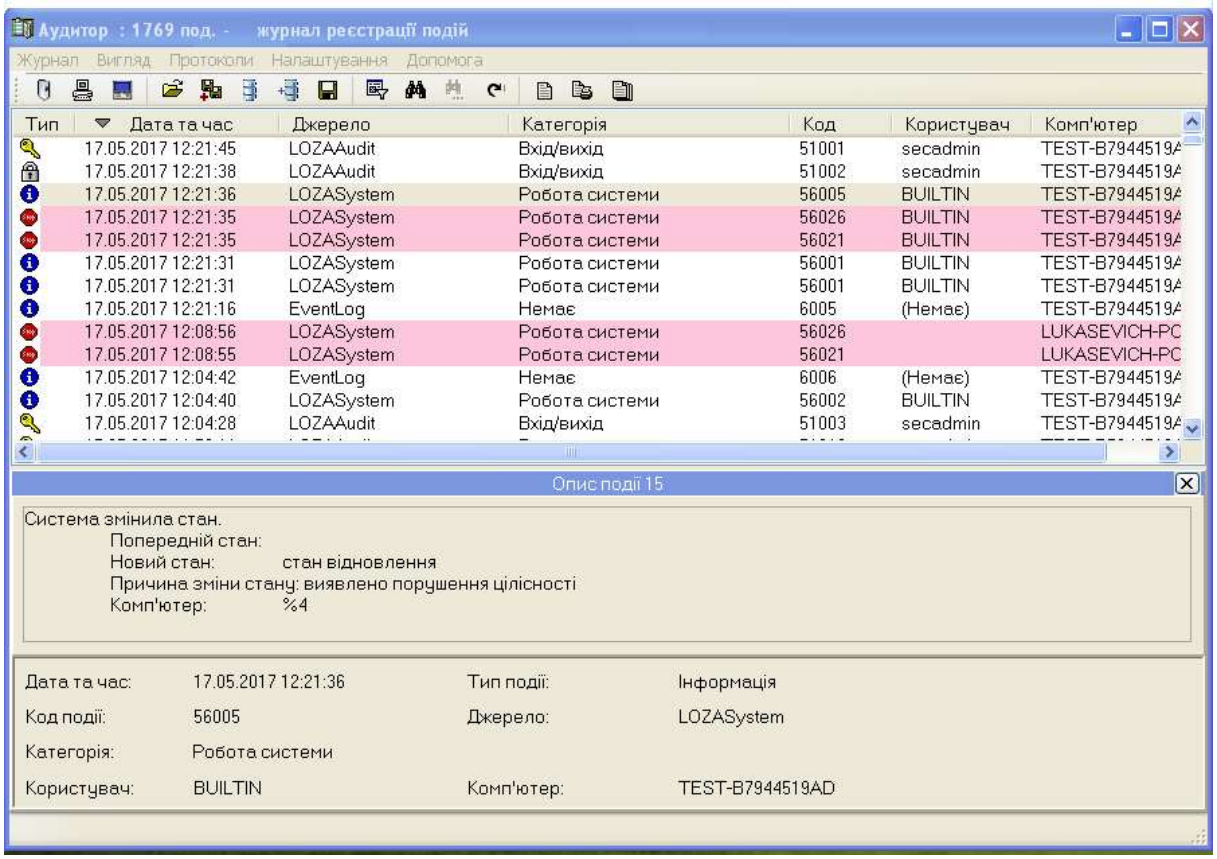

Рисунок 2.1– Головне вікно програми *Аудитор*

Тип події визначає її важливість або приналежність до аудиту. У таблиці 2.2 наведено можливі типи подій.

Таблиця 2.2 – Можливі типи подій

Позначка	Тип події	Значення
	Помилка	Важливі проблеми
	Попередження	Події, що не заважають роботі системи, але можуть викликати проблеми в майбутньому
	Інформація	Події, що описують успішне виконання операцій у системі
	Аудит успіхів	Події, що описують успішні дії користувачів, пов`язані з безпекою системи
	Аудит відмов	Події, що описують невдалі дії користувачів, пов`язані з безпекою системи

Джерело – це системний компонент чи прикладна програма, які зареєстрували подію в журналі.

Категорія – це група подій, логічно пов’язаних між собою. Категорія визначається в межах джерела.

Код події – це унікальний у межах джерела ідентифікатор події.

Опис події містить докладну інформацію про подію.

Опис події виводиться у нижній частині головного вікна програми (рисунок 2.1).

Користувач може закрити цю частину перегляду за допомогою кнопки ☒ у верхньому правому куті вікна перегляду або за допомогою пункту головного меню *Вигляд - Опис події*. Цей пункт функціонує як перемикач. Якщо опис події у даний момент відображається, то він його відключає. Якщо опис події не відображається, то він його повертає для відображення на дисплеї.

Крім того, переглянути опис події можна в окремому вікні, виконавши одну з таких дій:

– натиснути клавішу *Enter;*
– двічі натиснути клавішу миші;
– скористатись пунктом меню *Вигляд* – *Відомості*.

Для перегляду опису події призначене діалогове вікно *Відомості про подію* (рисунок 2.2).

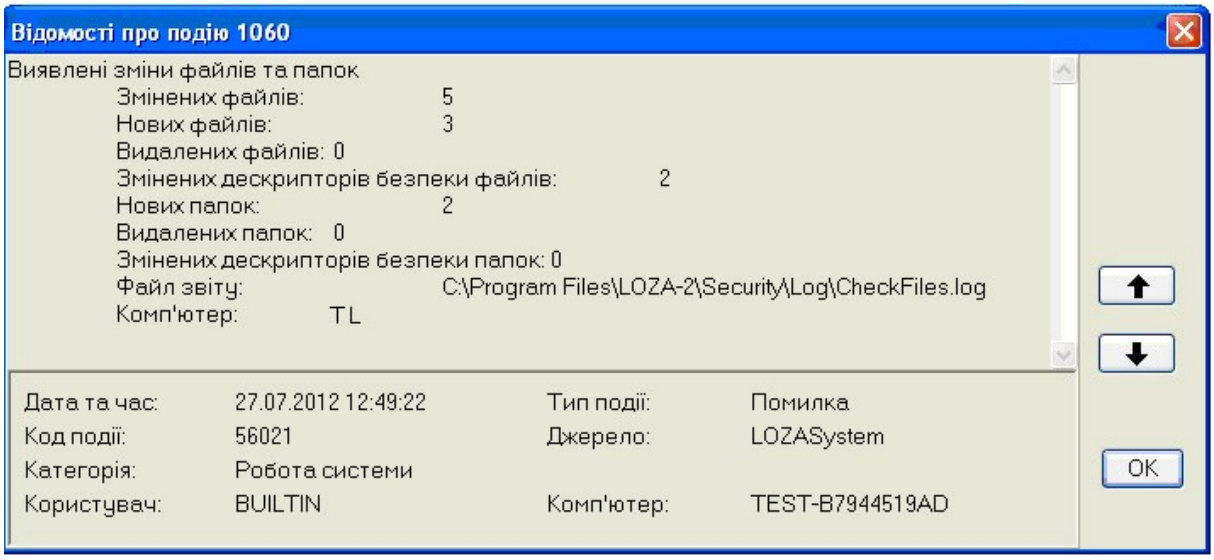

Рисунок 2.2 – Діалогове вікно для перегляду відомостей про подію

Не закриваючи цього вікна, за допомогою кнопок *Попередня подія* та *Наступна подія* можна переглянути відомості про інші події.

Порядок сортування подій можна встановити, натиснувши кнопку миші на заголовку відповідної колонки. При повторному натисканні на заголовок колонки встановлюється зворотний порядок сортування. У колонці, яка використовувалась для сортування, відображається маркер, що показує порядок сортування (▼ – прямий порядок сортування, ▲ – зворотний порядок сортування). Для одного й того ж значення колонки, по якій відбувається сортування, дані впорядковуються у хронологічному порядку. При відкритті журналу або резервної копії встановлюється хронологічна послідовність подій від новіших до старіших (для дати цей порядок вважається прямим).

Крім того, при перегляді можливо виділяти кольором небезпечні події. Це налаштування задається як параметр програми та зберігається доти, доки користувач його не змінить. Подія розглядається як небезпечна відповідно до поточних налаштувань системи.

2.2.1.2 Фільтрація подій

Фільтрація подій полягає у тому, що на екран виводиться не весь журнал (або резервна копія), а лише ті події, які задовольняють певним умовам.

Якщо фільтр встановлено, пункт меню ***Вигляд – Фільтр*** буде помічено.

Для того, щоб сформувати умови відбору подій, необхідно вибрати пункт меню ***Вигляд – Фільтр*** або натиснути кнопку  , після чого на екрані з'явиться діалогове вікно ***Фільтр*** (рисунок 2.3).

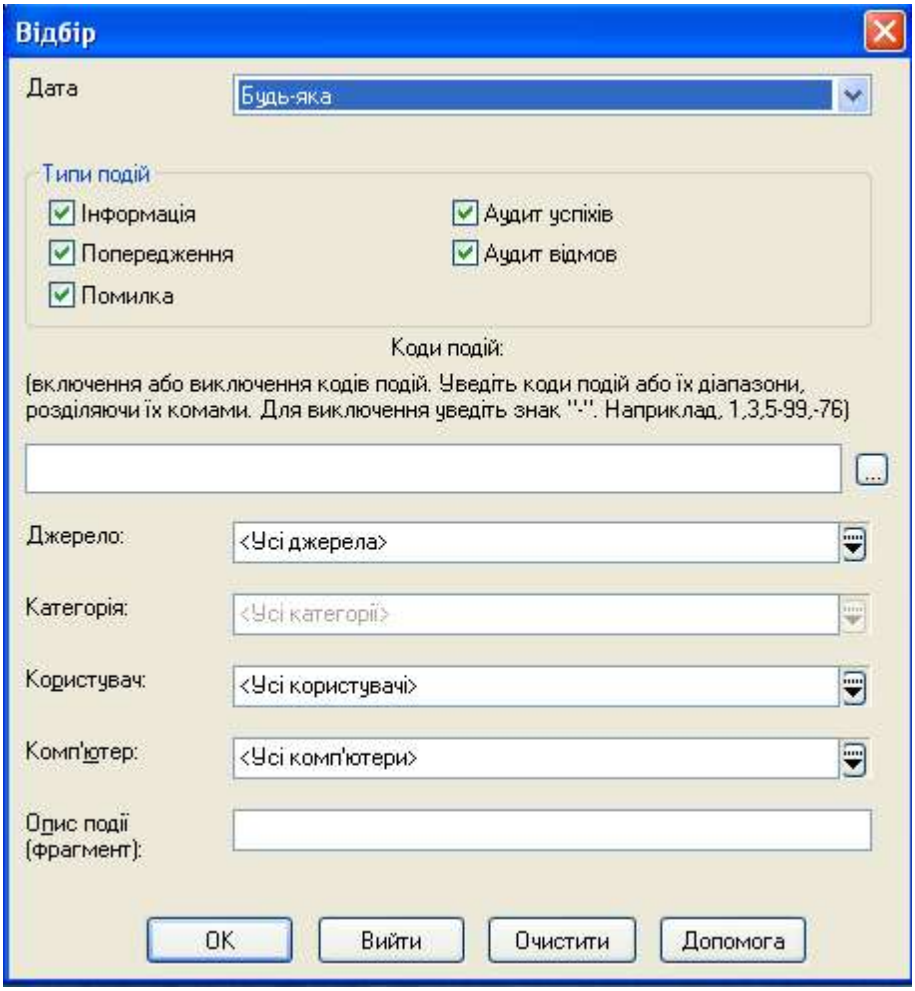

Рисунок 2.3 – Діалогове вікно для формування умов відбору подій

Для вибору інтервалу дат використовується пункт ***Дата***, який у розгорнутому вигляді наведено далі (рисунок 2.4).

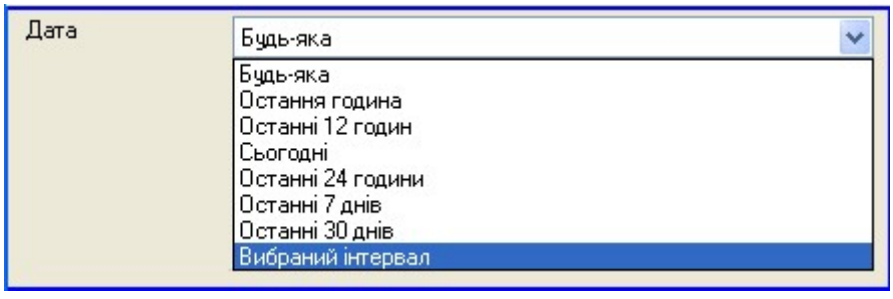

Рисунок 2.4 – Вибір дати при встановленні фільтру

Якщо вибрано останній з відображених (рисунок 2.4) режимів, то користувач має можливість встановити довільний інтервал за допомогою форми, представленої далі (рисунок 2.5).

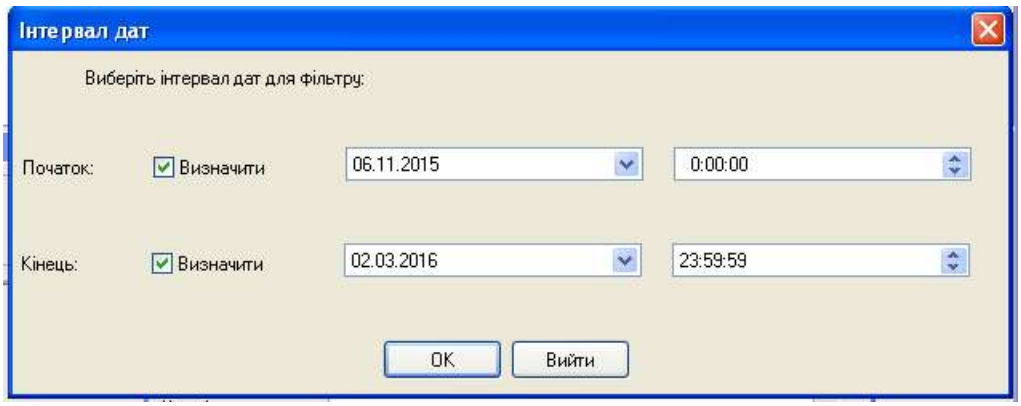

Рисунок 2.5 – Вибір довільного інтервалу дат при встановленні фільтру

Якщо визначено тільки початок інтервалу, то відбираються усі події, починаючи з вказаної дати. А якщо визначено тільки кінець інтервалу, то відбираються усі події, що відбулися до вказаної дати. Слід зазначити, що потрібно звертати увагу також на поля, що визначають час. При переході на нову дату для початку інтервалу автоматично встановлюється час 0:00:00 (початок доби), а при переході на нову дату для кінця інтервалу встановлюється час 23:59:59 (кінець доби).

На формі для встановлення відбору користувач має можливість також вказати:

– тип події (інформація, попередження, помилка, аудит успіхів, аудит відмов). Можна вибрати один або кілька типів подій;

– коди подій. Можна задати один або кілька інтервалів для включення або для виключення з відбору. Наприклад 1,3,5-99,-76 означатиме, що будуть відібрані події з кодами 1,3,5-99 за виключенням події з кодом 76. Для визначення списку кодів можна скористатись клавішею  , розташованою поряд з полем для уведення кодів. При натисканні цієї клавіші відображається наявний перелік кодів подій та їх опис (початкова частина). Приклад такого списку наведено далі (рисунок 2.7). Потрібні події можна шукати за контекстом (частиною опису). Відмітивши потрібні для відбору коди, ми отримаємо список у вікні для відбору;

– джерело (для відбору потрібно відмітити одне або кілька значень із списку, що випадає). Приклад такого відбору наведено далі (рисунок 2.6);

– якщо вибрано одне джерело, користувач має можливість вибрати категорію, що відповідає цьому джерелу подій (можна відмітити один або кілька рядків);

– аналогічно можна вибрати користувача та (або) комп'ютер;

– вказавши текст в полі *Опис події*, можна вказати фрагмент опису, який буде використовуватись для відбору.

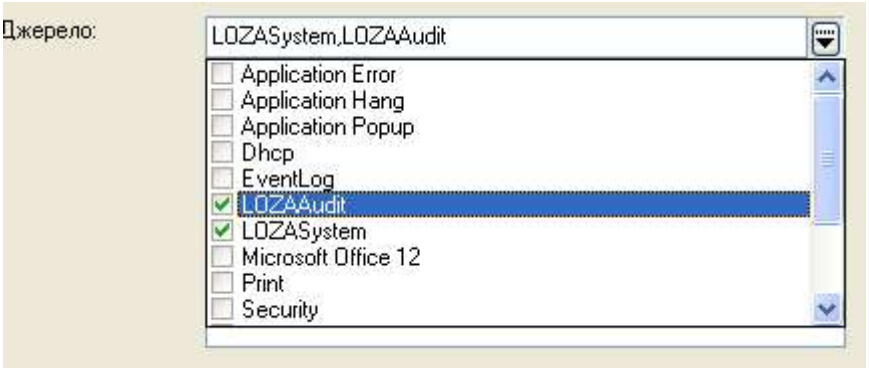

Рисунок 2.6 – Відбір по джерелу при встановленні фільтру

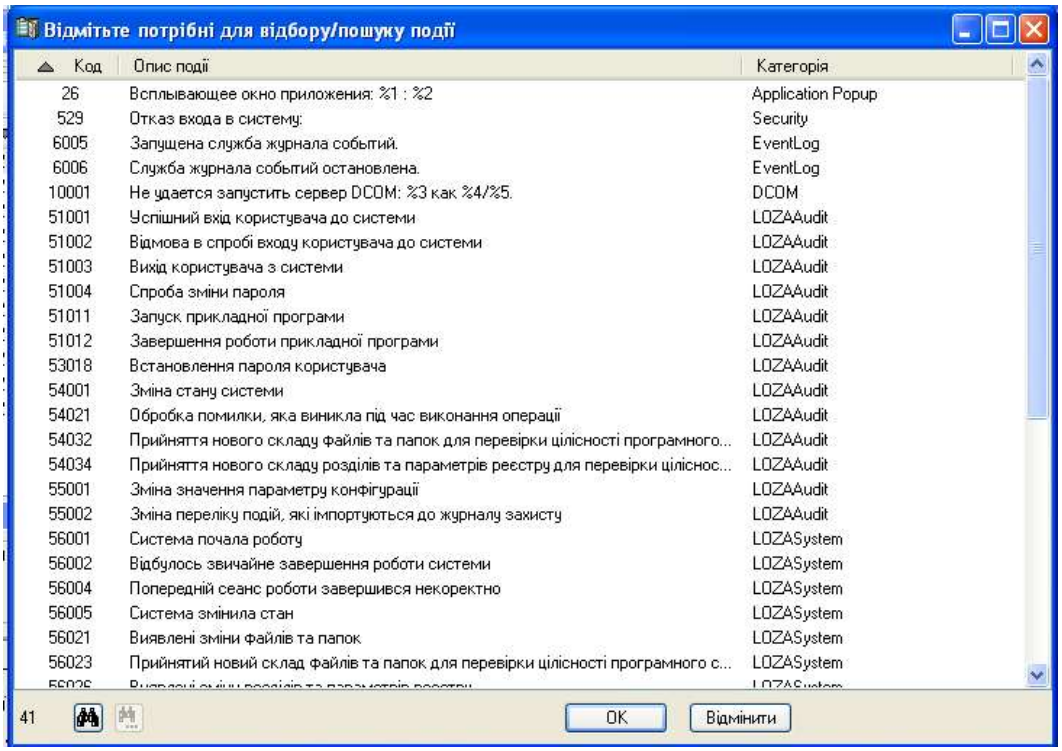

Рисунок 2.7 – Відбір кодів подій по їх опису при встановленні фільтру

Щоб поновити стандартні умови відбору подій (перегляд усього журналу), треба натиснути кнопку *Очистити* або виконати пункт головного меню *Вигляд - Усі події*.

2.2.1.3 Пошук подій

За допомогою пункту меню *Вигляд – Пошук* або кнопки  можна здійснювати пошук подій за певними умовами, які вказуються у діалоговому вікні, аналогічному вікну відбору, за виключенням пункту, що задає напрямок пошуку. Ці налаштування для пошуку наведено нижче (рисунок 2.8).

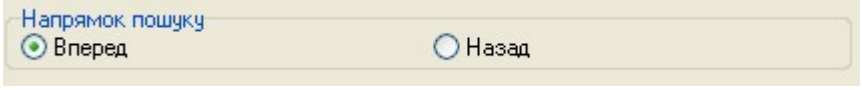

Рисунок 2.8 – Визначення напрямку пошуку подій

Після першого вдалого пошуку можна знайти наступну подію, яка задовольняє тим же умовам. Для цього можна скористатись пунктом меню *Вигляд – Пошук далі*, клавішею *F3* або кнопкою .

2.2.1.4 Налаштування зовнішнього вигляду вікна перегляду журналу реєстрації подій

Користувач може настроїти зовнішній вигляд вікна перегляду, зображеного на рисунку (рисунок 2.1). Він має можливість:

– змінити ширину та порядок колонок у верхній частині вікна перегляду за допомогою миші, перетягуючи колонки за їх заголовок або перетягуючи границі між колонками;

– змінити ширину колонок (у т.ч. зробити деякі з них невидимими) за допомогою пункту головного меню *Вигляд – Колонки*. Зовнішній вигляд цього вікна наведено далі (рисунок 2.9). Ширина колонок вказується у відсотках від загальної ширини вікна перегляду;

– змінити межу між верхньою та нижньою частинами вікна перегляду за допомогою миші;

– змінити шрифт у вікні перегляді за допомогою пункту меню *Параметри – Шрифт*.

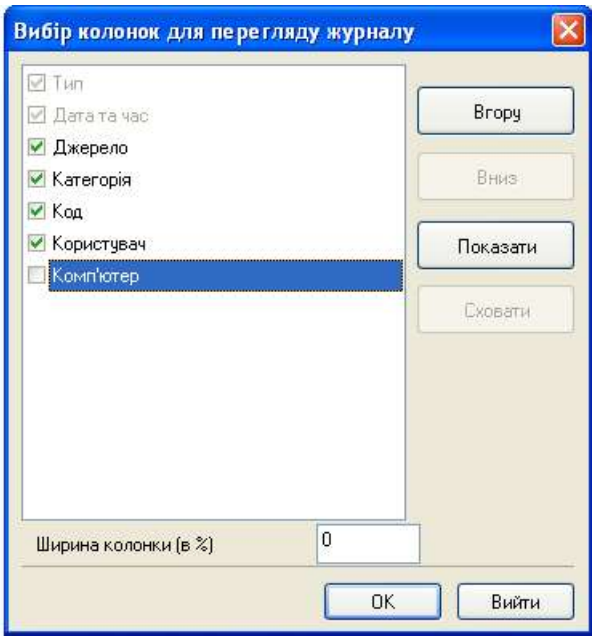

Рисунок 2.9 – Вікно для налаштування ширини колонок

2.2.1.5 Поновлення подій

Під час роботи на екрані відображаються записи, які знаходились в журналі реєстрації на момент запуску програми. Під час перегляду ці дані автоматично не поновлюються.

Для поновлення інформації необхідно скористатись пунктом меню *Вигляд – Поновити дані* або натиснути клавішу *F5*. Після цього нові події, які з'явились в журналі реєстрації, будуть відображені на екрані. При поновленні подій зберігаються раніше встановлені фільтр та впорядкованість подій (при повторному відкритті журналу реєстрації подій вони не зберігаються).

2.2.2 Створення резервних копій журналу та робота з ними

Програма *Аудитор* дозволяє зберігати журнал реєстрації у файлі та переглядати збережені журнали.

Збереження журналу здійснюється за допомогою пункту меню *Журнал – Зберегти як* або за допомогою кнопки  . Копія журналу зберігається в спеціальному форматі у файлі з розширенням **.lzl*, ім'я якого обирається користувачем. Програма пропонує зберігати копії журналів у папці *%LOZA%\SECURITY\LOG\BACKUP*.

Якщо при перегляді журналу було встановлено фільтр, то можна зберегти весь журнал або тільки відібрану його частину. Це визначається за допомогою спеціального запиту до користувача. Збереження відібраної частини журналу може бути корисним при аналізі певної групи подій.

Для перегляду збережених журналів використовуються пункти меню *Журнал – Відкрити* та *Журнал – Додати файл журналу* або відповідні кнопки  та  .

Пункт меню *Журнал – Відкрити* дозволяє відкрити збережений у файлі журнал, а пункт меню *Журнал – Додати файл журналу* додати інший файл журналу до вже відкритого. При додаванні даних до журналу перевіряється, щоб не було дублювання подій, тобто якщо у відкритому файлі та у файлі, що додається, є одні й ті ж події, вони будуть відображатись тільки один раз. Додати файл журналу можна як до іншої резервної копії, так і до поточного журналу реєстрації подій.

Під час роботи з відкритим файлом журналу пункт меню *Вигляд – Поновити дані* стає недоступним.

Пункт меню *Журнал – Журнал реєстрації* та кнопка  дозволяють повернутись до поточного журналу реєстрації після роботи з резервними копіями журналу реєстрації.

Програма *Аудитор* може бути запущена також автономно від інших програмних засобів системи ЛОЗА-1. Для цього при запуску програми потрібно вказати параметр запуску /LOZADoNotRegister. У такому випадку можна переглядати та роздруковувати лише раніше створені резервні копії журналу реєстрації подій.

2.2.3 Формування та друк звіту та протоколів

Програма *Аудитор* дозволяє формувати такі документи:

– звіт про небезпечні події (містить інформацію щодо функціонування системи протягом дня);

– протокол друку документів (містить відомості про друк документів);

– протокол подій за вибором (містить події, які відбираються за вказаними критеріями, наприклад, певні типи подій, категорії подій, дії певного користувача та ін.).

Форми звіту про небезпечні події та протоколу друку наведено далі, а також у документі "Загальний опис системи". Форма протоколу подій за вибором наведена далі.

Звіт про небезпечні події зберігається як текстовий файл (формат Txt), а протоколи зберігаються у форматі RTF, для їхнього перегляду та друку можна використовувати, наприклад, текстовий процесор MS Word або стандартну програму Windows WordPad.

2.2.3.1 Звіт про помилки та небезпечні події

Звіт про помилки та небезпечні події може бути сформований за допомогою пункту меню *Протоколи – Звіт про помилки та небезпечні події* або кнопки  (цей самий звіт формується автоматично під час роботи системи у випадку виникнення відповідних подій). Цей пункт доступний тільки при перегляді поточного журналу реєстрації подій (не резервної копії).

Звіт містить загальну інформацію про функціонування системи протягом дня, а саме:

– час початку роботи системи;

– зафіксовані небезпечні події (із зазначенням джерела, коду та часу подій) або їхню відсутність;

– зафіксовані помилки (із зазначенням джерела, коду та часу подій) або їхню відсутність.

Якщо для будь-якого джерела та коду зафіксовано більше 10-ти подій, то час вказується для перших 9-ти подій та останньої. Інші замінюються "…".

Події відносяться до небезпечних згідно з параметрами конфігурації `перелік небезпечних подій` та `вважати помилки небезпечними подіями`.

Форма звіту наведена нижче (рисунок 2.10).

```
                              ЛОЗА-1
      Звіт про помилки та небезпечні події
            за 08.08.2015
          Комп'ютер TL

Час початку роботи: 09:09:55

Протягом сеансу роботи в системі:

 небезпечні події не зафіксовані

 зафіксовані помилки (7):
   LOZASystem\56021 (09:43:17, 10:08:59);
   LOZASystem\56026 (10:09:12);
   LOZASystem\56099 (10:09:21, 10:27:58, 10:29:21, 11:53:02).

Звіт сформований: 04.12.2019 11:55:35
```

Рисунок 2.10 – Звіт про помилки та небезпечні події

2.2.3.2 Протокол друку документів

Протокол друку формується за допомогою пункту меню *Протоколи – Протокол друку* або кнопки  .

Він може формуватися за датою або за інтервалом дат, що визначається в діалоговому вікні *Протокол за* (рисунок 2.11).

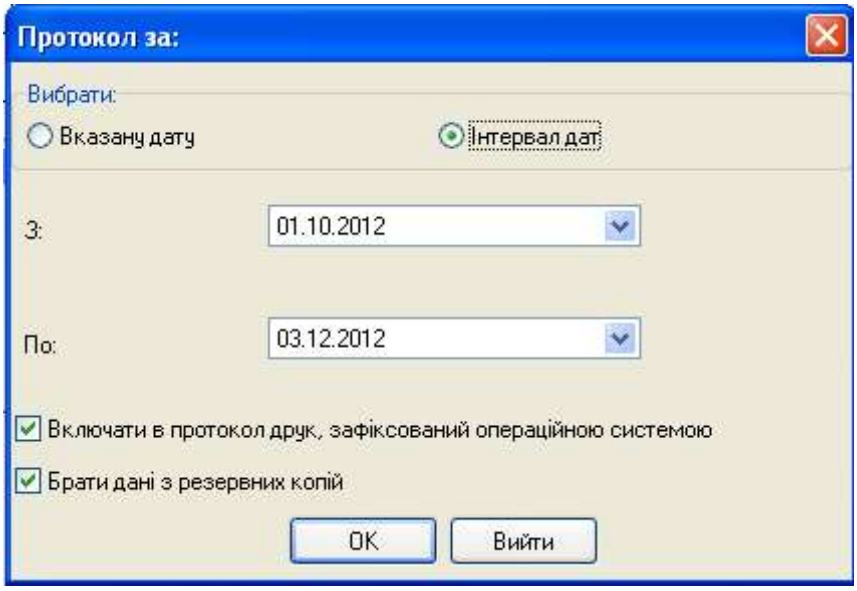

Рисунок 2.11 – Діалогове вікно для формування умов відбору до протоколу друку

До протоколу друку включається інформація, яка міститься в подіях *Спроба друку екранної форми LOZAAudit* (категорія *Доступ до вихідних форм*, код 52004) та *Спроба друку документа* (категорія *Доступ до документів*, код 58004) джерела *LOZAAudit*, а також друк, зафіксований операційною системою, якщо користувач вказав відповідне налаштування на формі, зображеній на рисунку (рисунок 2.11). Для того, щоб в протокол був включений друк, зафіксований операційною системою, потрібно виконати певні умови:

– настроїти в Windows протоколювання події друку (див. п.2.2 документа *Інструкція системного адміністратора*);

– включити імпорт цієї події в журнал системи ЛОЗА (див. п.3.2.7.2.1.3 цього документа).

Крім того, у протокол можна включити дані з резервних копій, якщо встановити відмітку так, як зображено на рисунку (рисунок 2.11).

Протокол друку містить загальну інформацію про друк документів для зазначеної дати чи інтервалу дат, а саме:

– обрану дату або інтервал дат;
– загальну кількість надрукованих документів;
– загальну кількість надрукованих аркушів документів.

Протокол друку містить також детальну інформацію про кожний документ для зазначеної дати або інтервалу дат, а саме:

– дату (підзаголовок);
– час друку документа;
– ім’я користувача, що друкував документ;
– принтер, на якому надруковано документ;
– комп'ютер, з якого друкувався документ;
– назву документа;
– гриф документа (для події 58004);
– обліковий номер документа (для події 58004);
– загальну кількість надрукованих аркушів;
– кількість примірників (для події 58004) .

Протокол друку містить також для кожної дати підсумковий рядок із кількістю аркушів, надрукованих протягом дня. Форма протоколу наведена нижче (рисунок 2.12).

Протокол друку документів

з 01.12.2018 по 31.12.2018

Надруковано документів: …

(Усього аркушів: …)

N п/п	Час	Користу-вач	Комп'ю-тер	Принтер	Документ			Надруковано	
					назва	гриф	обліко-ковий №	аркушів, усього	примір-ників
	08.12.2018								
1	16:06:09	UserDoc	TL	Bullzip PDF Printer	D:\Тест\ Наказ №111	таєм-но	122	2	1
2	16:06:10	UserDoc	TL	Bullzip PDF Printer	Microsoft Word - Документ в Word_00002709			2	
3	16:08:21	UserDoc	TL	Bullzip PDF Printer	D:\Тест\ Розпоряд-ження	таєм-но	123	2	1

Рисунок 2.12 – Протокол друку документів

2.2.3.3 Протокол подій за вибором

Протокол подій за вибором формується за допомогою пункту меню *Протоколи – Протокол за вибором* або кнопки  . Діалогове вікно *Протокол за вибором* (рисунок 2.13) аналогічне вікну *Фільтр*, воно дозволяє сформувати умови відбору подій для протоколу.

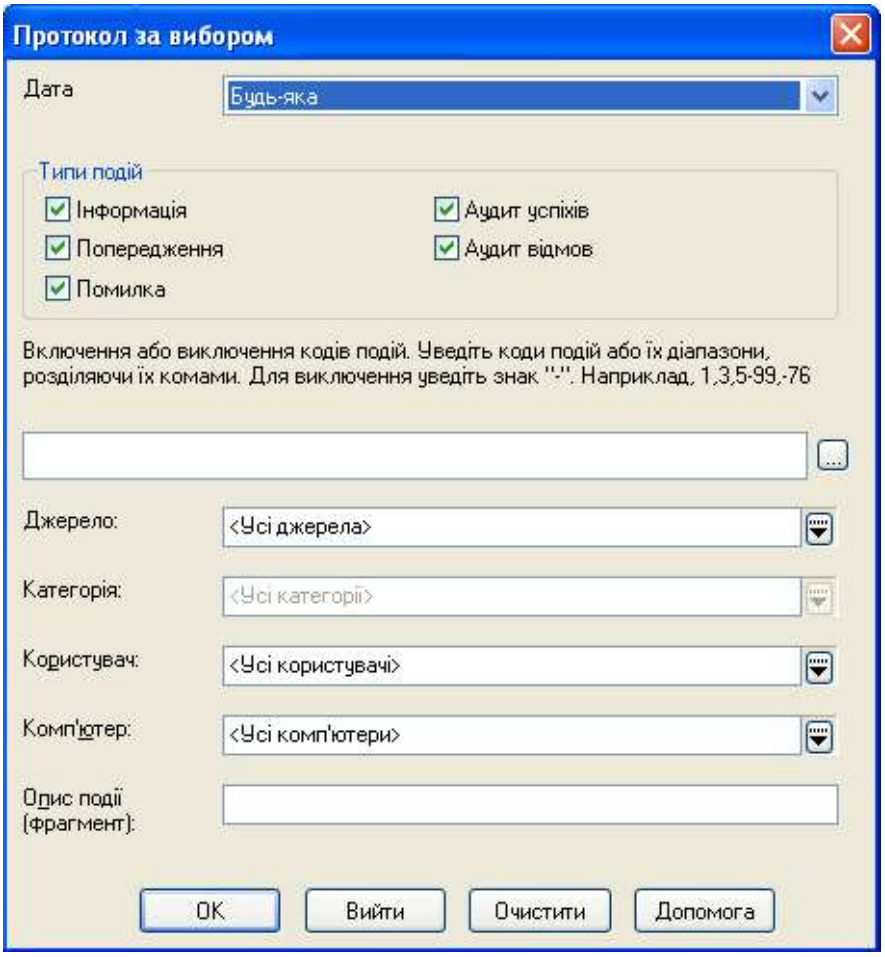

Рисунок 2.13 – Діалогове вікно для формування умов відбору для протоколу за вибором

Поля цього вікна заповнюються аналогічно полям вікна ***Фільтр*** (див. п. 2.2.1.2).

Якщо умови відбору не вказувати, до протоколу будуть включені усі події, що містяться в журналі, з повним описом подій. Форма протоколу наведена далі (рисунок 2.14).

Протокол подій

з 08.12.2018 по 31.12.2018

Зафіксовано подій: …

N п/п	Час	Тип події	Джерело	Категорія	Код події	Користувач	Комп'ютер	Опис події
08.12.2018								
1	16:02:26	Аудит відмов	Security	Вход/ выход	529	SYSTEM	TL	Отказ входа в систему: Причина: неизвестное имя пользователя или неверный пароль Пользователь: secadmin Домен: BUGH Тип входа: 3 Процесс входа: NtLmSsp Пакет проверки: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Рабочая станция: BUGH
2	…							

Рисунок 2.14 – Протокол подій за вибором

3 Програма *Керування захистом*

3.1 Призначення та основні функції

Програма *Керування захистом* призначена для вирішення завдань, які пов'язані із встановленням повноважень користувачів, визначенням параметрів конфігурації системи та ін.

Програма *Керування захистом* надає такі можливості:

– перегляд та коригування даних про користувачів;
– перегляд та коригування значень параметрів конфігурації системи.

3.2 Робота із програмою

У таблиці 3.1 наведено структуру головного меню програми.

Таблиця 3.1 – Структура головного меню програми *Керування захистом*

Меню	Підменю	Дія
Дані	Користувачі	Робота з переліком користувачів
	Групи	Робота з переліком груп користувачів
	Рівні доступу	Робота з переліком рівнів доступу
	Захищені процеси	Робота з переліком захищених процесів
	Захищені папки	Робота з переліком захищених папок
	Зареєстровані диски USB Flash	Робота з переліком зареєстрованих дисків USB Flash
Конфігурація – Загальні параметри	Реєстрація подій – Видалення резервних копій	Встановлення параметрів видалення резервних копій журналу реєстрації подій
	Робота з документами – Політика документів	Встановлення політики документів
	Доступ до технологічної інформації	Встановлення повноважень адміністраторів
	Політика облікових записів – Політика паролів	Встановлення параметрів політики паролів
	Політика облікових записів – Політика блокування облікового запису	Встановлення параметрів політики блокування облікового запису
	Вхід до системи	Встановлення параметрів входу до системи
	Шаблони користу-вача – Зареєстровані диски USB Flash	Визначення шаблону даних користувача для дисків USB Flash
	Безпечне видалення інформації	Встановлення рівня доступу, для якого відбувається безпечне видалення інформації для захищених папок та зареєстрованих дисків USB Flash (за допомогою процедури Wipe)
Конфігурація –	Реєстрація подій –	Параметри журналу реєстрації подій

Меню	Підменю	Дія
Параметри комп'ютера	Параметри журналу	
	Реєстрація подій – Політика аудиту	Встановлення політики аудиту
	Реєстрація подій – Імпорт подій	Встановлення переліку подій, що імпортуються з журналів Windows
	Реєстрація подій – Небезпечні події	Встановлення переліку небезпечних подій
	Реєстрація подій – Реакція на небезпечні події	Встановлення параметрів, що визначають реакцію системи на виникнення небезпечних подій
	Додаткові засоби адміністрування	Встановлення параметрів додаткових засобів адміністрування
	Перевірка цілісності	Встановлення параметрів перевірки цілісності
	Робота з документами – Шаблони та надбудови	Встановлення переліку дозволених шаблонів та надбудов для MS Word та MS Excel
	Робота з документами – Диски для зберігання документів	Встановлення дисків для зберігання документів
	Робота з документами – Небезпечні команди Excel	Встановлення небезпечних команд Excel
	Робота з документами – Небезпечні команди Word	Встановлення небезпечних команд Word
	Робота з документами – Захист друку документів	Встановлення параметрів захисту друку документів
	Робота з документами – Захист експорту документів	Встановлення параметрів захисту експорту документів
	Політики знімних дисків	Встановлення політик знімних дисків
	Заборона друку	Встановлення параметрів заборони друку
	Заборонені програми	Встановлення переліку заборонених програм
	Тимчасові файли	Встановлення переліку тимчасових папок та файлів
	Системні облікові записи	Встановлення переліку системних облікових записів
	Довірені процеси	Визначення довірених процесів. Довірені процеси – це процеси, які не контролюються файловим драйвером ЛОЗИ для запобігання конфліктів з антивірусними програмами. Вони матимуть доступ до захищених папок користувачів і до папок самої ЛОЗИ. Для кожного процесу вказується відповідний

Меню	Підменю	Дія
		йому файл
	Обробка подій	В системі передбачена можливість обробки певних подій. Для цих подій вказуються функції обробки та їх параметри
Конфігурація – Встановлення значення за умовчанням		Встановлення значення за умовчанням для параметрів конфігурації
Конфігурація – Імпорт параметрів конфігурації		Збереження визначених параметрів конфігурації системи ЛОЗА у спеціальному файлі
Конфігурація – Експорт параметрів конфігурації		Встановлення визначених параметрів конфігурації системи ЛОЗА відповідно до значень, збережених раніше у спеціальному файлі
Налаштування	Панелі інструментів	Налаштування панелі інструментів
Налаштування	Розташування за умовчанням	Розташування панелей інструментів за умовчанням (якщо настройка, яку виконав користувач, не задовольняє його)
Допомога	Зміст	Перегляд файлу допомоги
	Про програму	Перегляд інформації про програму

При виборі пункту головного меню ***Дані*** додатково з'являються пункти головного меню ***Коригування*** та ***Вигляд***, склад яких описано нижче.

3.2.1 Робота з переліком користувачів системи

При виборі пункту меню ***Дані – Користувачі*** чи натисканні кнопки з'являється вікно з переліком усіх користувачів системи. Кожний рядок переліку містить ім'я, повне ім'я та опис користувача, список ролей, які він виконує в системі, рівень його допуску та типи ключових дисків (основного та резервного). У головному меню додатково з'являються пункти ***Коригування*** та ***Вигляд***. Робота з даними про користувачів проводиться у вікні ***Дані – Користувачі*** (рисунок 3.1).

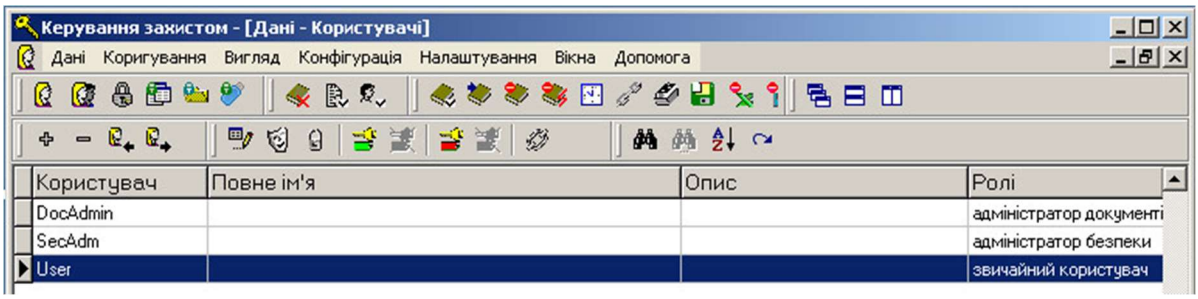

Рисунок 3.1 – Вікно для роботи з даними про користувачів

Можливості, які надає програма при роботі з даними про користувачів, наведено в таблиці 3.2.

Таблиця 3.2

Пункт меню	Кнопка	Дія
Коригування – Додати користувача		Введення даних про нового користувача
Коригування – Видалити користувача		Видалення даних про користувача
Коригування – Ролі користувача		Коригування ролей вибраного користувача
Коригування – Рівень допуску		Коригування рівня допуску вибраного користувача
Коригування – Властивості користувача		Встановлення та коригування властивостей користувача
Коригування – Перейменувати користувача		Перейменування користувача
Коригування – Змінити пароль		Зміна пароля користувача
Коригування – Ототожнити користувача		Ототожнення користувача з одного комп’ютера на іншому
Коригування – Ініціалізувати ключовий диск		Ініціалізація ключового диска
Коригування – Видалити ключовий диск		Видалення ключового диска
Коригування – Ініціалізувати резервний ключовий диск		Ініціалізація резервного ключового диска
Коригування – Видалити резервний ключовий диск		Видалення резервного ключового диска
Коригування – Імпортувати перелік користувачів		Імпорт переліку користувачів з резервного носія для проведення відновлення бази облікових записів
Коригування – Експортувати перелік користувачів		Експорт переліку користувачів для ототожнення на інших комп’ютерах та створення резервних копій бази облікових записів
Коригування – Змінити пароль		Зміна пароля користувача
Вигляд – Пошук		Пошук користувача за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортування даних		Сортування даних за вказаними полями (ім’ям або повним описом). Сортування також відбувається при натискання на заголовок колонки. При повторному натисканні відбувається сортування у зворотному порядку.
Вигляд – Поновити дані		Поновлення даних про користувачів

3.2.1.1 Введення даних про нового користувача

Для того, щоб ввести дані про нового користувача, треба послідовно ввести:

- ім’я користувача;
- властивості користувача;
- перелік ролей, які він буде виконувати в системі;

– рівень допуску користувача;
– ініціалізувати ключовий диск (за необхідності).

Дані про нового користувача вводяться за допомогою пункту меню *Коригування – Додати користувача* або кнопки  , після чого на екрані послідовно з'являються відповідні вікна.

Кнопка **>>** в усіх вікнах дозволяє продовжити введення даних, кнопка **<<** – повернутись в попереднє вікно, кнопка *Відмінити* – відмінити введення даних, кнопка *Зберегти* – зберегти дані про нового користувача.

При введенні нового користувача він автоматично включається до відповідних груп Windows (див. п. 5.1.2.2 документа "Загальний опис системи").

3.2.1.1.1 Введення імені та властивостей користувача

Для введення імені та властивостей нового користувача призначено діалогове вікно *Властивості користувача* (рисунок 3.2).

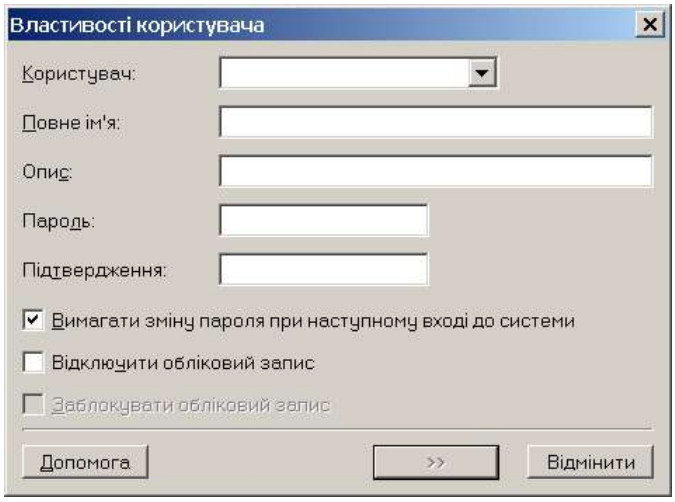

Рисунок 3.2 – Діалогове вікно для введення імені та властивостей нового користувача

У полі *Користувач* вводиться унікальне ім'я, під яким користувач буде працювати в системі.

При цьому ім'я можна ввести вручну чи вибрати одне з імен зі списку, що випадає в цьому полі. До цього списку включаються ті користувачі, для яких було створено облікові записи в Windows та які не були занесені до переліку користувачів системи та службових користувачів.

У полях *Повне ім'я, Опис, Вимагати зміну пароля при наступному вході до системи, Відключити обліковий запис* при наявності відповідного облікового запису в Windows відображаються дані, які було вказано під час його створення. Усі коригування будуть автоматично внесені до облікового запису користувача в Windows.

Якщо для користувача не був створений обліковий запис у Windows, він буде створений автоматично на основі введених даних.

3.2.1.1.2 Введення ролей користувача

Для введення ролей нового користувача призначено діалогове вікно *Ролі користувача* (рисунок 3.3).

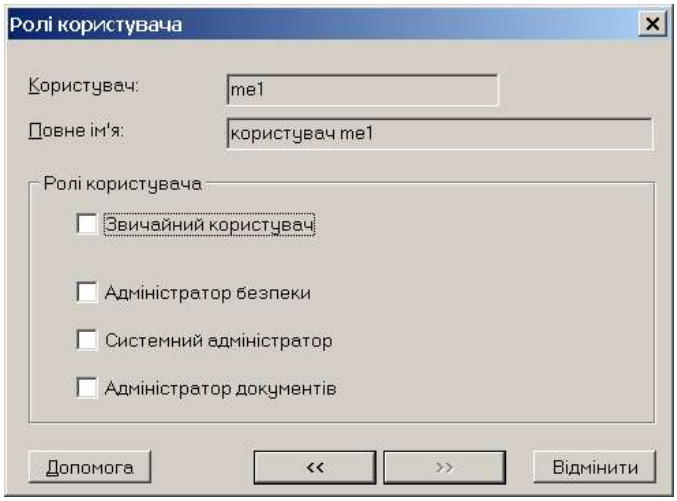

Рисунок 3.3 – Діалогове вікно для введення ролей нового користувача

Для встановлення ролей користувача в групі *Ролі користувача* встановлюються відмітки, що відповідають ролям, які виконує користувач у системі. Роль звичайного користувача не суміщається з жодною з адміністративних ролей, адміністративні ролі можна суміщати.

3.2.1.1.3 Введення рівня допуску користувача

Для введення рівня допуску нового користувача призначено діалогове вікно *Рівень допуску користувача* (рисунок 3.4).

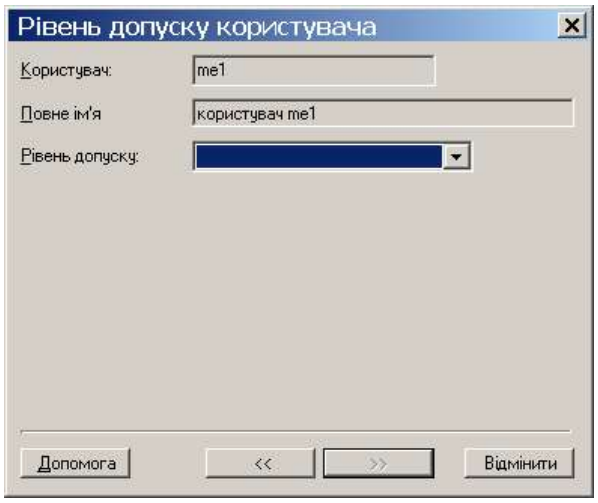

Рисунок 3.4 – Діалогове вікно для введення рівня допуску нового користувача

У полі *Рівень допуску* вводиться рівень допуску користувача. При цьому він обирається з переліку рівнів доступу серед рівнів доступу, відмічених для використання.

3.2.1.1.4 Ініціалізація ключового диска користувача

Для ініціалізації ключового диска нового користувача (у випадку, коли встановлений параметр конфігурації `Перевіряти ключовий диск під час входу до Windows`) призначене діалогове вікно *Ініціалізація ключового диска* (рисунок 3.5).

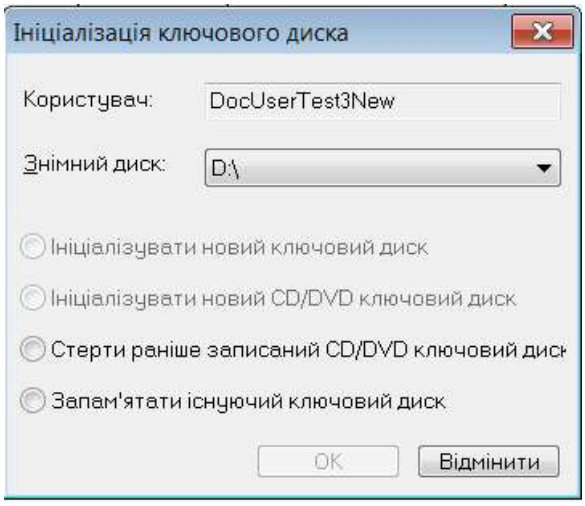

Рисунок 3.5 – Вікно для ініціалізації ключового диска

Якщо вибрано CD/DVD диск, то в залежності від його стану можуть бути доступними різні опції. Для неініціалізованного диску доступним буде пункт *ініціалізувати новий CD/DVD ключовий диск*, для ініціалізованного CD/DVD диску в будь-якому випадку буде доступним пункт *стерти раніше записаний CD/DVD ключовий диск*, в у випадку, коли на ньому вже є ключ користувача ЛОЗИ, буде доступним також пункт *запам'ятати існуючий ключовий диск*. Слід пам'ятати, що ініціалізація CD/DVD диску або його очистка можлива лише у випадку, коли обладнання це допускає.

Один і той же ключовий диск може використовуватись на різних комп'ютерах. Під час створення ключового диска на першому комп'ютері необхідно обрати опцію *ініціалізувати новий ключовий диск*, під час створення ключового диска на інших комп'ютерах – опцію *запам'ятати існуючий ключовий диск*.

3.2.1.2 Видалення даних про користувача

Для того, щоб видалити дані про користувача, треба вибрати відповідний рядок у переліку користувачів і скористатись пунктом меню *Коригування – Видалити користувача* або натиснути кнопку  . Після підтвердження дані про користувача буде видалено.

Не можна видалити дані про користувача, якщо він є єдиним адміністратором безпеки.

При видаленні користувача він автоматично видаляється з усіх груп Windows, до яких його було автоматично включено.

При видаленні користувача за бажанням можна видалити і його обліковий запис у Windows.

3.2.1.3 Коригування даних про користувача

Для того, щоб скоригувати властивості користувача, треба вибрати відповідний рядок у переліку користувачів та скористатись пунктом меню *Коригування – Властивості користувача* або натиснути кнопку  . Крім того, коригування поточного користувача відбувається при натисканні клавіші Enter (або подвійному натискання лівої клавіші миші). Коригування відбувається за правилами, наведеними в п. 3.2.1.1.1).

Для того, щоб скоригувати перелік ролей користувача, треба вибрати відповідний рядок у переліку користувачів та скористатись пунктом меню

Коригування – Ролі користувача або натиснути кнопку  . Коригування відбувається за правилами, наведеними в п. 3.2.1.1.2).

Роль *Звичайний користувач* не суміщається з жодною з адміністративних ролей, тому для встановлення ролі *Звичайний користувач* треба зняти відмітки з усіх адміністративних ролей, і навпаки – для встановлення адміністративних ролей треба зняти відмітку з ролі *Звичайний користувач*.

Для того, щоб скоригувати рівень допуску введеного користувача, треба вибрати відповідний рядок у переліку користувачів та скористатись пунктом меню *Коригування – Рівень допуску* або натиснути кнопку  . Коригування відбувається за правилами, наведеними в п. 3.2.1.1.3.

3.2.1.4 Ініціалізація ключового диска

Для того, щоб ініціалізувати ключовий диск треба вибрати відповідний рядок у переліку користувачів, вставити відповідний знімний диск та скористатись пунктом меню *Коригування – Ініціалізувати ключовий диск* або натиснути кнопку  .

Процес ініціалізації описано в п. 3.2.1.1.4.

3.2.1.5 Видалення ключового диска

Для видалення ключового диска треба вибрати відповідний рядок у переліку користувачів та скористатись пунктом меню *Коригування – Видалити ключовий диск* або натиснути кнопку  .

Після підтвердження інформацію про ключовий диск буде видалено.

3.2.1.6 Ініціалізація резервного ключового диска

Резервний ключовий диск є рівноправним з основним і може ініціалізуватись для будь-якого користувача системи.

Для того, щоб ініціалізувати ключовий диск, треба вибрати відповідний рядок у переліку користувачів, вставити відповідний знімний диск та скористатись пунктом меню *Коригування – Ініціалізувати резервний ключовий диск* або натиснути кнопку  . Проведення ініціалізації описано в п. 3.2.1.1.4.

3.2.1.7 Видалення резервного ключового диска

Для видалення резервного ключового диска треба вибрати відповідний рядок у переліку користувачів та скористатись пунктом меню *Коригування – Видалити резервний ключовий диск* або натиснути кнопку  .

Після підтвердження інформацію про ключовий диск буде видалено.

3.2.1.8 Ототожнення користувача

У тому випадку, коли користувачу необхідно працювати з документами, які зберігаються на знімному носії, на декількох комп'ютерах можливе виникнення ситуації, коли дозволи на доступ до документа або бази документів, надані на одному комп'ютері, не матимуть сили на іншому (незалежно від того, чи використовує користувач на різних комп'ютерах одне й те ж ім'я). Причина полягає в тому, що в списках доступу документа та бази документів (які зберігаються разом із документами та базами) зазначається не ім'я користувача, а його унікальний ідентифікатор – SID. Ці ідентифікатори ніколи не повторюються, тому на різних комп'ютерах один і той же користувач матиме різні SID'и. Для того, щоб запобігти такій ситуації і надати користувачам можливість працювати з документами на різних комп'ютерах,

використовується *ототожнення* користувачів. Порядок встановлення ототожнень для користувачів простіше всього пояснити за допомогою простого приклада.

Припустимо, що користувач працює на комп'ютерах *К1* та *К2* під іменем *User1*. Нижче описаний процес встановлення ототожнення.

1) На комп'ютері *К1* за допомогою пункту меню *Коригування – Експортувати перелік користувачів* відкрити перелік користувачів та виконати його експорт на знімний носій. Припустимо, що адміністратор безпеки назвав файл з експортованим переліком *К1_Users* (якщо файл було отримано на ранніх версіях і він має cds - формат, то його потрібно перетворити у *.sdt,* для цього потрібно використати спеціальну утиліту для перетворення, див. п. 5.2).

2) На комп'ютері *К2* за допомогою пункту меню *Дані – Користувачі* відкрити перелік користувачів.

3) Встановити ототожнення для користувача *User1*. Для цього треба виконати такі дії:

обрати пункт меню *Коригування – Ототожнити користувача* або натиснути кнопку  :

у діалозі вказати файл *К1_Users.sdt*;

обрати в переліку рядок *К1\User1*;

зберегти ототожнення.

4) Повторити кроки 1) – 3) для встановлення ототожнення „у зворотному напрямку" (тобто виконати експорт переліку користувачів на комп'ютері *К2* та встановити ототожнення на комп'ютері *К1*).

При перегляді списку користувачів можна використовувати такі можливості:

при натисканні на заголовок колонки дані впорядковуються у відповідності зі значенням даних у колонці. Повторне натискання приводить до сортування у зворотному порядку. Наявність та напрямок сортування відображаються за допомогою стрілки у заголовку колонки  ;

при натисканні клавіші Enter (або подвійне натискання лівої клавіші миші) можно перейти до редагування властивостей поточного користувача;

за допомогою миші можна встановлювати потрібну ширину колонок (вона буде зберігатись, доки користувач її не змінить).

3.2.2 Робота з переліком груп користувачів

При виборі пункту меню *Дані – Групи* чи натисканні кнопки  з'являється вікно з переліком усіх груп користувачів системи. Кожний рядок переліку містить ім'я групи, опис групи та список її членів. У головному меню додатково з'являються пункти *Коригування* та *Вигляд*. Робота з даними про групи користувачів проводиться у вікні *Дані – Групи* (рисунок 3.6).

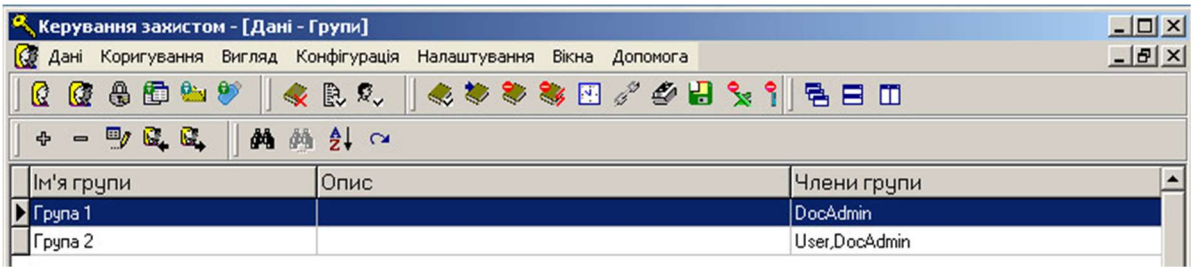

Рисунок 3.6 – Вікно для роботи з даними про групи користувачів

Можливості, які надає програма при роботі з даними про групи користувачів, наведено в таблиці 3.3.

Таблиця 3.3

Пункт меню	Кнопка	Дія
Коригування – Додати групу		Введення даних про нову групу користувачів
Коригування – Видалити групу		Видалення даних про групу користувачів
Коригування – Коригувати групу		Коригування даних про групу користувачів
Коригування – Перейменувати групу		Перейменування групи користувачів
Коригування – Імпортувати перелік груп користувачів		Імпорт переліку користувачів з резервного носія для проведення відновлення бази облікових записів
Коригування – Експортувати перелік груп користувачів		Експорт переліку груп користувачів для створення резервних копій бази облікових записів
Вигляд – Пошук		Пошук групи за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за іменем групи. Сортування за значенням довільної колонки відбувається при натисканні на заголовок колонки
Вигляд – Поновити дані		Поновлення даних про групи користувачів

3.2.2.1 Введення даних про нову групу користувачів

Дані про нову групу користувачів вводяться за допомогою пункту меню *Коригування – Додати групу* або кнопки за допомогою діалогового вікна *Нова група* (рисунок 3.7).

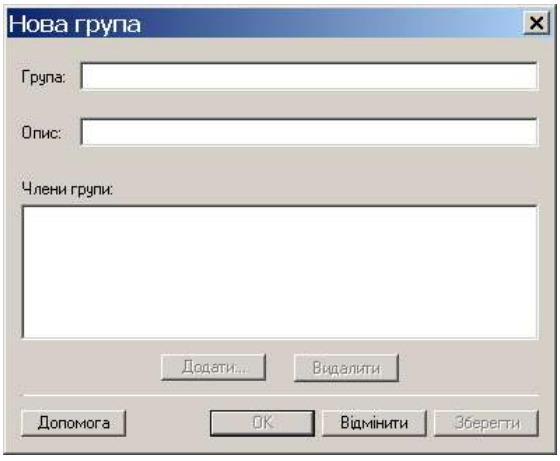

Рисунок 3.7 – Діалогове вікно для введення нової групи користувачів

За допомогою кнопки *Додати* можна включити до групи одного або декількох нових членів. Для цього призначене діалогове вікно *Користувачі* (рисунок 3.8). Користувачі розташовані в алфавітному порядку. Можна відмітити один або кілька рядків для включення в групу.

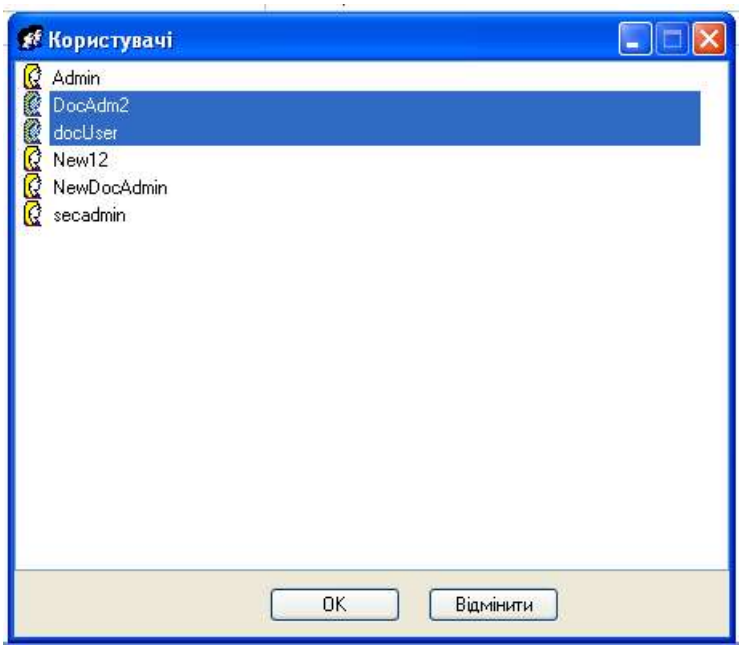

Рисунок 3.8 – Діалогове вікно для включення до групи нового члена

За допомогою кнопки *Видалити* можна видалити з групи одного або декількох її членів.

3.2.2.2 Видалення даних про групу користувачів

Для того, щоб видалити дані про групу користувачів, треба вибрати відповідний рядок у переліку груп користувачів і скористатись пунктом меню *Коригування – Видалити групу* або натиснути кнопку . Після підтвердження дані про групу користувачів буде видалено.

3.2.2.3 Коригування даних про групу користувачів

Для того, щоб скоригувати дані про групу користувачів, треба вибрати відповідний рядок у переліку груп та скористатись пунктом меню *Коригування – Коригувати групу* або натиснути кнопку . Крім того, коригування поточної групи відбувається при натисканні клавіші Enter (або подвійному натискання лівої клавіші миші). Коригування відбувається за правилами, наведеними в п. 3.2.2.1.

3.2.3 Робота з переліком рівнів доступу

При виборі пункту меню *Дані – Рівні доступу* чи натисканні кнопки з'являється вікно з переліком усіх можливих рівнів доступу системи. Кожний рядок переліку назв рівня, гриф та відмітку про використання в системі. У головному меню додатково з'являються пункти *Коригування* та *Вигляд*. Робота з переліком рівнів доступу проводиться у вікні *Дані – Рівні доступу* (рисунок 3.9).

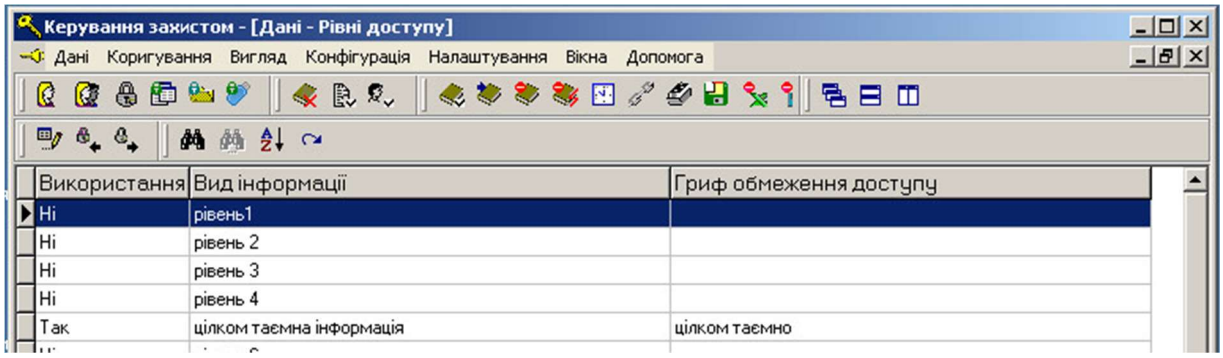

Рисунок 3.9 – Вікно для роботи з переліком рівнів доступу

Можливості, які надає програма при роботі з переліком рівнів доступу, наведено в таблиці 3.4.

Таблиця 3.4

Пункт меню	Кнопка	Дія
Коригування – Коригувати рівень доступу		Коригування рівня доступу
Коригування – Імпортувати перелік рівнів доступу		Імпорт переліку рівнів доступу з резервного носія для проведення відновлення
Коригування – Експортувати перелік рівнів доступу		Експорт переліку рівнів доступу користувачів для створення резервних копій
Вигляд – Пошук		Пошук рівня доступу за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за кодом. Сортування за значенням довільної колонки відбувається при натисканні на заголовок колонки
Вигляд – Поновити дані		Поновлення переліку рівнів доступу

3.2.3.1 Коригування рівня доступу

Для того, щоб скоригувати рівень доступу, треба вибрати відповідний рядок у переліку рівнів доступу та скористатись пунктом меню *Коригування – Коригувати рівень доступу* або натиснути кнопку (рисунок 3.10). Крім того, коригування поточного рівня доступу відбувається при натисканні клавіші Enter (або подвійному натисканні лівої клавіші миші).

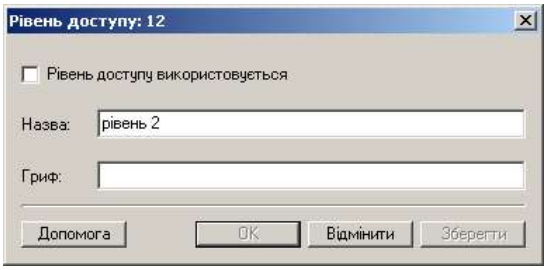

Рисунок 3.10 – Діалогове вікно для коригування рівня доступу

3.2.4 Робота з переліком захищених процесів

При виборі пункту меню *Дані – Захищені процеси* чи натисканні кнопки  з'являється вікно з переліком захищених процесів системи. Кожний рядок переліку містить ім'я процесу та контрольну суму файлу, а також довідково список доступу для процесу. У головному меню додатково з'являються пункти *Коригування* та *Вигляд*. Робота з даними про захищені процеси проводиться у вікні *Дані – Захищені процеси* (рисунок 3.11).

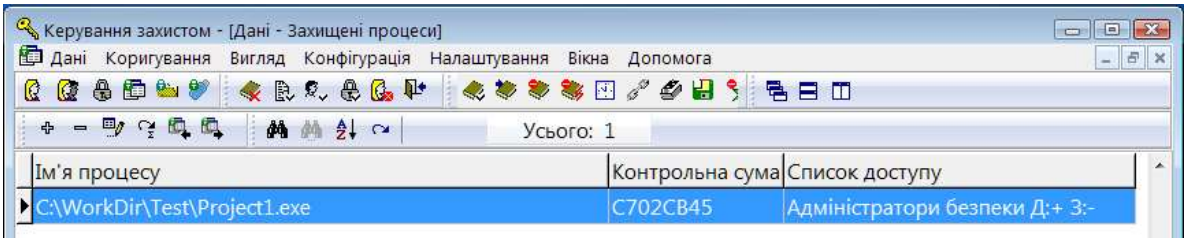

Рисунок 3.11 – Вікно для роботи з даними про захищені процеси

Можливості, які надає програма при роботі з даними про захищені процеси, наведено в таблиці 3.5.

Таблиця 3.5

Пункт меню	Кнопка	Дія
Коригування – Додати захищений процес		Введення даних про новий захищений процес
Коригування – Видалити захищений процес		Видалення даних про захищений процес
Коригування – Коригувати дані про захищений процес		Коригування даних про захищений процес
Коригування – Поновити контрольну суму		Поновлення контрольної суми файлу
Коригування – Імпортувати перелік захищених процесів		Імпорт переліку захищених процесів з резервного носія для проведення відновлення
Коригування – Експортувати перелік захищених процесів		Експорт переліку захищених процесів для створення резервних копій
Вигляд – Пошук		Пошук захищеного процесу за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за іменем процесу або за значенням довільної колонки відбувається при натисканні на заголовок колонки
Вигляд – Поновити дані		Поновлення даних про захищені процеси

3.2.4.1 Введення даних про новий захищений процес

Дані про новий захищений процес вводяться за допомогою пункту меню *Коригування – Додати захищений процес* або кнопки  . Ім'я нового захищеного процесу вводиться або вибирається у діалоговому вікні *Відкрити файл з переліком процесів* (рисунок 3.12).

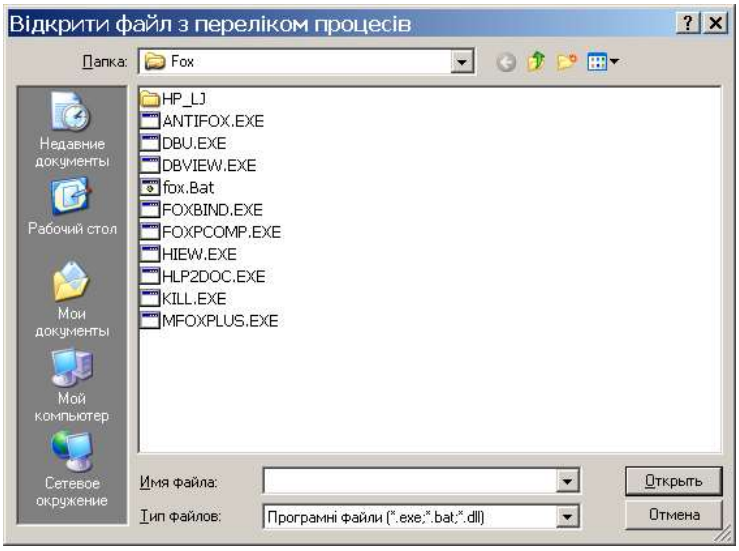

Рисунок 3.12 – Діалогове вікно для введення імені нового захищеного процесу

Після натискання кнопок ***Открыть – ОК*** з'являється діалогове вікно для введення даних про захищений процес – списку доступу та списку аудиту (рисунок 3.13).

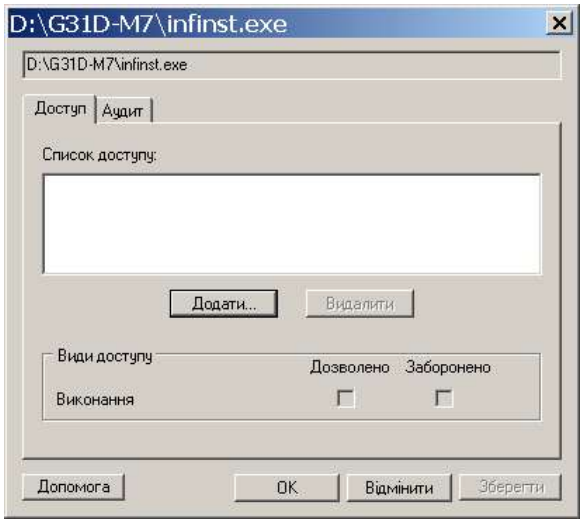

Рисунок 3.13 – Діалогове вікно для введення списку доступу захищеного процесу

За допомогою кнопки ***Додати*** можна додати користувача чи групу користувачів до списку доступу цього процесу. Відмітка у полі ***Дозволено*** означає, що користувачу або групі користувачів дозволено доступ до цього процесу на виконання, відмітка у полі ***Заборонено*** означає, що доступ заборонений.

За допомогою кнопки ***Видалити*** можна видалити користувача із списку доступу обраного процесу.

На сторінці ***Аудит*** можна ввести список аудиту процесу (рисунок 3.14).

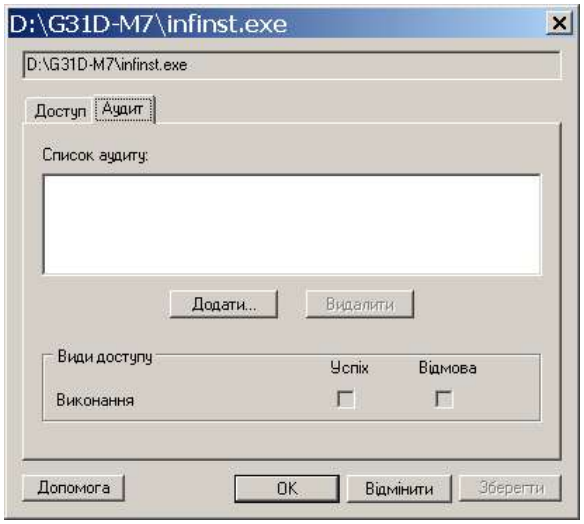

Рисунок 3.14 – Діалогове вікно для введення списку аудиту захищеного процесу

За допомогою кнопки *Додати* можна додати користувача чи групу користувачів до списку аудиту цього процесу. Відмітка у полі *Успіх* означає, що для користувача або групи користувачів буде встановлено аудит успішного доступу на виконання цього процесу, відмітка у полі *Відмова* означає, що буде встановлено аудит відмов у доступі до цього процесу.

За допомогою кнопки *Видалити* можна видалити користувача із списку аудиту процесу.

Слід пам'ятати, що загальна кількість захищених шляхів (тобто захищених процесів та захищених папок) не може перевищувати 1000. У разі перевищення користувач отримає відповідне повідомлення і об'єкт не буде додаватись до списку.

3.2.4.2 Видалення даних про захищений процес

Для того, щоб видалити дані про захищений процес, треба вибрати відповідний рядок у переліку захищених процесів і скористатись пунктом меню *Коригування – Видалити захищений процес* або натиснути кнопку . Після підтвердження дані про захищений процес буде видалено.

3.2.4.3 Коригування даних про захищений процес

Для того, щоб скоригувати дані про захищений процес, треба вибрати відповідний рядок у переліку захищених процесів та скористатись пунктом меню *Коригування – Коригувати дані про захищений процес* або натиснути кнопку . Крім того, коригування поточного процесу відбувається при натисканні клавіші Enter (або подвійному натискання лівої клавіші миші). Коригування відбувається за правилами, наведеними в п. 3.2.4.1.

3.2.5 Робота з переліком захищених папок

При виборі пункту меню *Дані – Захищені папки* чи натисканні кнопки з'являється вікно з переліком захищених папок системи. Кожний рядок переліку містить ім'я папки, рівень доступу та ознаку, що вказує на наявність/відсутність обмежень для процесів, які можуть отримати доступ до цієї папки. У головному меню додатково з'являються пункти *Коригування* та *Вигляд*. Робота з даними про захищені папки проводиться у вікні *Дані – Захищені папки* (рисунок 3.15).

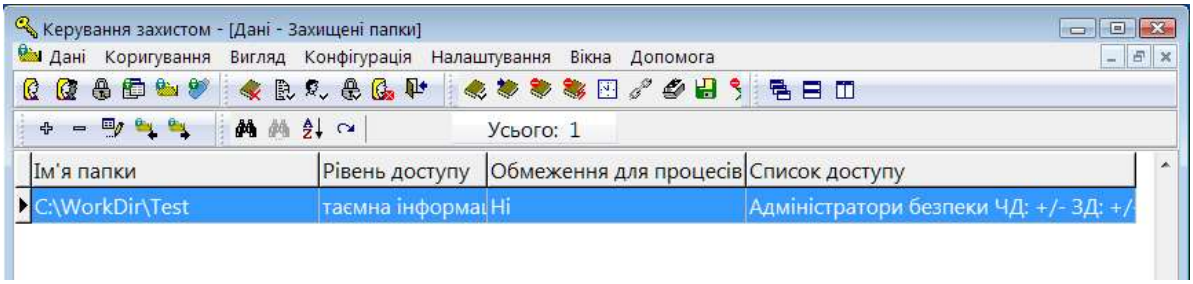

Рисунок 3.15– Вікно для роботи з даними про захищені папки

Можливості, які надає програма під час роботи з даними про захищені папки, наведено в таблиці 3.6.

Таблиця 3.6

Пункт меню	Кнопка	Дія
Коригування – Додати дані про захищену папку		Введення даних про нову захищену папку
Коригування – Видалити дані про захищену папку		Видалення даних про захищену папку
Коригування – Коригувати дані про захищену папку		Коригування даних про захищену папку
Коригування – Імпортувати перелік захищених папок		Імпорт переліку захищених папок з резервного носія для проведення відновлення переліку захищених папок
Коригування – Експортувати перелік захищених папок		Експорт переліку захищених папок для створення резервних копій переліку захищених папок
Вигляд – Пошук		Пошук захищеної папки за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за іменем папки. Сортування за значенням довільної колонки відбувається при натисканні на заголовок колонки
Вигляд – Поновити дані		Поновлення даних про захищені папки

3.2.5.1 Введення даних про нову захищену папку

Дані про нову захищену папку вводяться за допомогою пункту меню *Коригування – Додати захищену папку* або кнопки . Ім'я нової захищеної папки вводиться або вибирається у діалоговому вікні *Обзор папок* (рисунок 3.16).

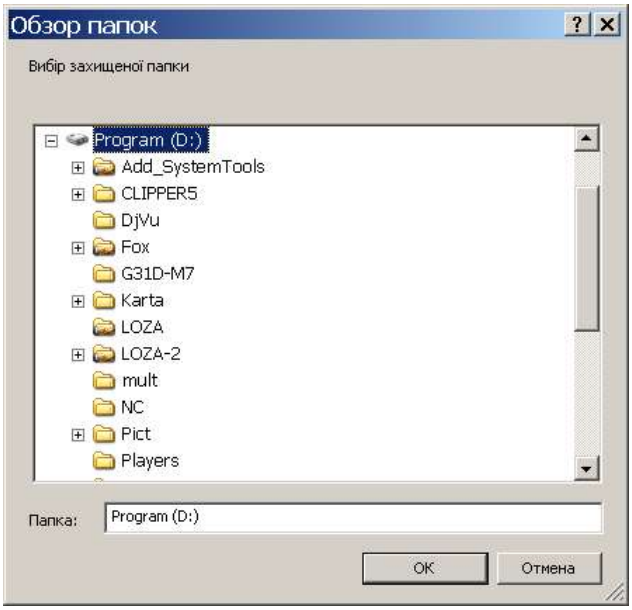

Рисунок 3.16 – Діалогове вікно для введення імені нової захищеної папки

Після натискання кнопки ***OK*** з'являється діалогове вікно для введення даних про захищену папку – загальних параметрів, списку доступу та списку аудиту (рисунок 3.17).

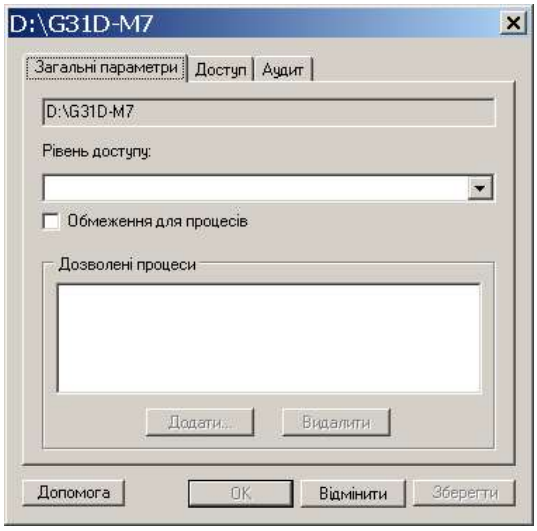

Рисунок 3.17 – Діалогове вікно для введення загальних параметрів для захищеної папки

У полі ***Рівень доступу*** вводиться рівень доступу папки – максимальний рівень доступу інформації, яка може зберігатись в цій папці. При цьому він обирається з переліку рівнів доступу серед рівнів доступу, відмічених для використання.

Відмітка у полі ***Обмеження для процесів*** вказує на наявність переліку процесів, які можуть отримати доступ до цієї папки.

У разі, коли встановлена відмітка у полі ***Обмеження для процесів,*** формується перелік дозволених процесів. За допомогою кнопки ***Додати*** можна додати процес до переліку дозволених процесів, за допомогою кнопки ***Видалити*** можна видалити процес із переліку дозволених процесів.

На сторінці ***Доступ*** можна ввести список доступу обраної папки (рисунок 3.18).

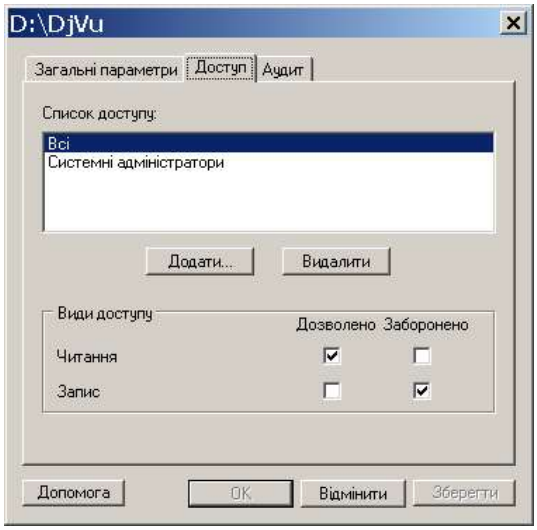

Рисунок 3.18 – Діалогове вікно для введення списку доступу захищеної папки

За допомогою кнопки ***Додати*** можна додати користувача чи групу користувачів до списку доступу папки. Відмітка у полі ***Дозволено*** означає, що користувачу або групі користувачів дозволено відповідний доступ до цієї папки, відмітка у полі ***Заборонено*** означає, що доступ заборонений.

За допомогою кнопки ***Видалити*** можна видалити користувача із списку доступу обраної папки.

На сторінці ***Аудит*** можна ввести список аудиту обраної папки (рисунок 3.19).

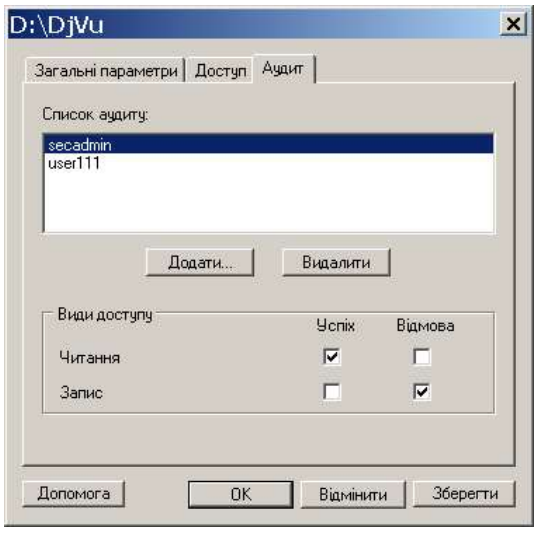

Рисунок 3.19 – Діалогове вікно для введення списку аудиту захищеної папки

За допомогою кнопки ***Додати*** можна додати користувача чи групу користувачів до списку аудиту папки. Відмітка у полі ***Успіх*** означає, що для користувача або групи користувачів буде встановлено аудит успішного доступу на читання та/або запис до цієї папки, відмітка у полі ***Відмова*** означає, що буде встановлено аудит відмов у доступі на читання та/або запис до цієї папки.

За допомогою кнопки ***Видалити*** можна видалити користувача із списку аудиту обраної папки.

Слід пам’ятати, що загальна кількість захищених шляхів (тобто захищених папок та захищених процесів) не може перевищувати 1000. У разі перевищення користувач отримає відповідне повідомлення і об’єкт не буде додаватись до списку.

3.2.5.2 Видалення даних про захищену папку

Для того, щоб видалити дані про захищену папку, треба вибрати відповідний рядок у переліку захищених папок і скористатись пунктом меню *Коригування – Видалити захищену папку* або натиснути кнопку  . Після підтвердження дані про захищену папку буде видалено. При цьому користувач може видалити саму захищену папку та весь її вміст після підтвердження (рисунок 3.20).

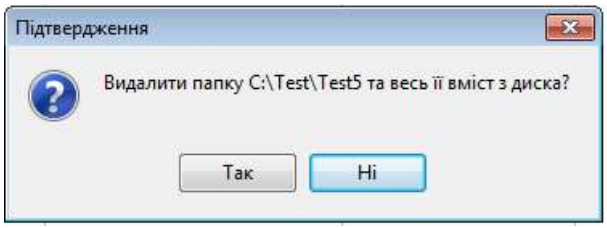

Рисунок 3.20 – Діалогове вікно для підтвердження видалення захищеної папки з її вмістом

Це підтвердження буде продубльовано ще одним (рисунок 3.21).

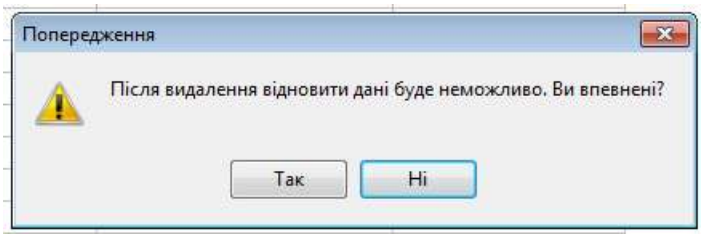

Рисунок 3.21– Повторне повідомлення для підтвердження видалення захищеної папки з її вмістом

Але для фактичного видалення потрібно ввести слово "Видалити" у спеціальному вікні (рисунок 3.22).

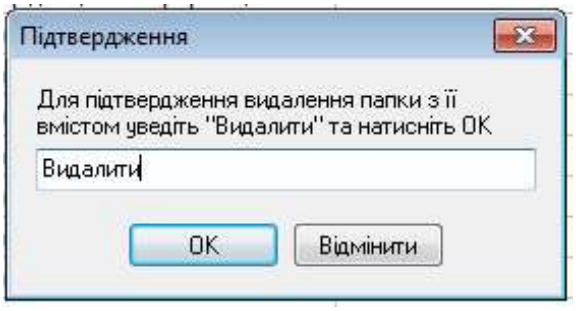

Рисунок 3.22 – Підтвердження фактичного видалення захищеної папки з її вмістом

Такі засоби потрібні, щоб запобігти випадковому видаленню папки, бо після цього відновити її зміст вже неможливо (якщо папка видалялась безпечно, тобто за допомогою процедури Wipe).

3.2.5.3 Коригування даних про захищену папку

Для того, щоб скоригувати дані про захищену папку, треба вибрати відповідний рядок у переліку захищених папок та скористатись пунктом меню *Коригування – Коригувати дані про захищену папку* або натиснути кнопку  . Крім того, коригування поточної захищеної папки відбувається при натисканні клавіші Enter (або подвійному натискання лівої клавіші миші). Коригування відбувається за правилами, наведеними в п. 3.2.5.1.

3.2.6 Робота з переліком зареєстрованих дисків USB Flash

При виборі пункту меню *Дані – Зареєстровані диски USB Flash* чи натисканні кнопки  з'являється вікно з переліком зареєстрованих дисків USB Flash. Кожний рядок переліку містить серійний номер, рівень доступу та ознаку, що вказує на наявність/відсутність обмежень для процесів, які можуть отримати доступ до цього диска. У головному меню додатково з'являються пункти *Коригування* та *Вигляд*. Робота з даними про зареєстровані диски USB Flash проводиться у вікні *Дані – Зареєстровані диски USB Flash* (рисунок 3.23).

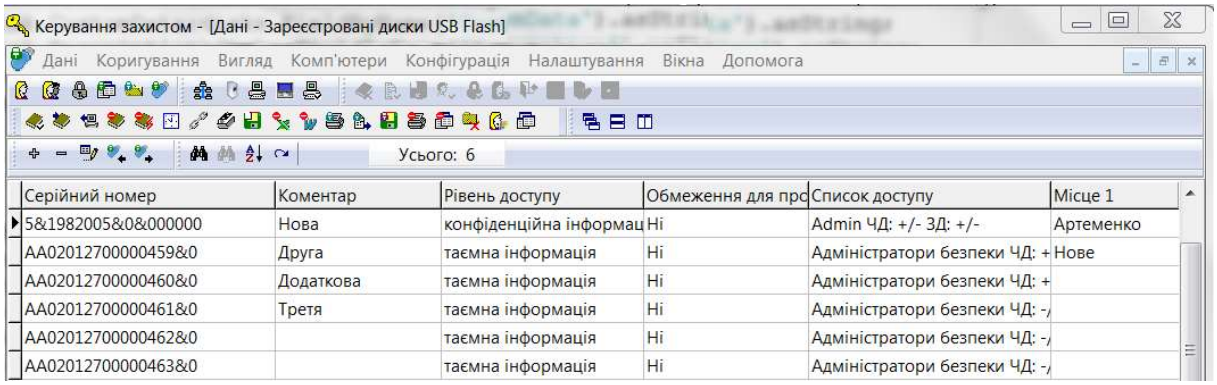

Рисунок 3.23 – Вікно для роботи з даними про зареєстровані диски USB Flash

Можливості, які надає програма під час роботи з даними про зареєстровані диски USB Flash, наведено в таблиці 3.7.

Таблиця 3.7

Пункт меню	Кнопка	Дія
Коригування – Додати дані про знімний диск		Введення даних про новий зареєстрований диск USB Flash
Коригування – Видалити дані про знімний диск		Видалення даних про зареєстрований диск USB Flash
Коригування – Коригувати дані про знімний диск		Коригування даних про зареєстрований диск USB Flash
Коригування – Імпортувати перелік знімних дисків		Імпорт переліку зареєстрованих дисків USB Flash з резервного носія для проведення відновлення переліку зареєстрованих дисків USB Flash
Коригування – Експортувати перелік знімних дисків		Експорт переліку зареєстрованих дисків USB Flash для створення резервних копій переліку зареєстрованих дисків USB Flash
Вигляд – Пошук		Пошук зареєстрованого диску USB Flash за вказаними умовами

Пункт меню	Кнопка	Дія
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за серійним номером. Для сортування за значеннями будь-якої колонки потрібно натиснути на її заголовок. Повторне натискання приводить до сортування у зворотному порядку
Вигляд – Поновити дані		Поновлення даних про зареєстровані диски USB Flash

3.2.6.1 Введення даних про новий зареєстрований диск USB Flash

Дані про новий зареєстрований диск USB Flash вводяться за допомогою пункту меню *Коригування – Додати дані про знімний диск* або кнопки  . Новий диск, який необхідно зареєструвати, вибирається у діалоговому вікні *Диски USB Flash* (рисунок 3.24).

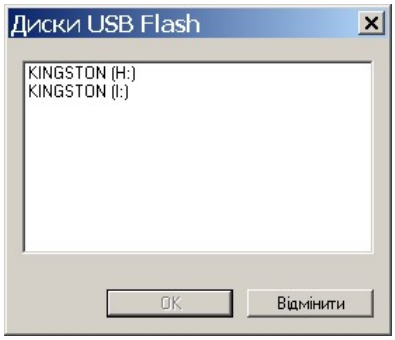

Рисунок 3.24 – Діалогове вікно для вибору знімного диска

Після натискання кнопки *OK* з'являється діалогове вікно для введення даних про диск – загальних параметрів, списку доступу та списку аудиту (рисунок 3.25).

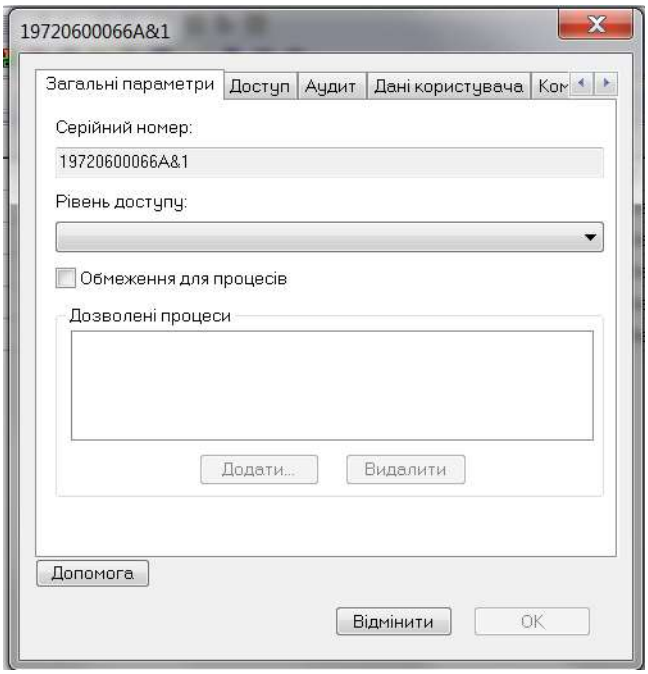

Рисунок 3.25 – Діалогове вікно для введення загальних параметрів для диска

У полі *Рівень доступу* вводиться рівень доступу диска – максимальний рівень доступу інформації, яка може зберігатись на цьому диску. При цьому він обирається з переліку рівнів доступу серед рівнів доступу, відмічених для використання.

Відмітка у полі *Обмеження для процесів* вказує на наявність переліку процесів, які можуть отримати доступ до цього диска.

У разі, коли встановлена відмітка у полі *Обмеження для процесів,* формується перелік дозволених процесів. За допомогою кнопки *Додати* можна додати процес до переліку дозволених процесів, за допомогою кнопки *Видалити* можна видалити процес із переліку дозволених процесів.

На сторінці *Доступ* можна ввести список доступу обраного диска (рисунок 3.26).

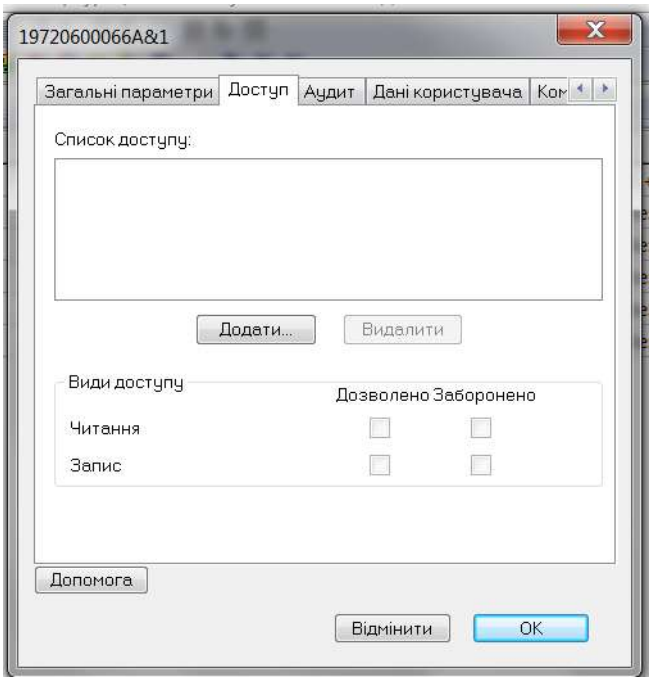

Рисунок 3.26 – Діалогове вікно для введення списку доступу диска

За допомогою кнопки *Додати* можна додати користувача чи групу користувачів до списку доступу диска. Відмітка у полі *Дозволено* означає, що користувачу або групі користувачів дозволено відповідний доступ до цього диска, відмітка у полі *Заборонено* означає, що доступ заборонений.

За допомогою кнопки *Видалити* можна видалити користувача із списку доступу обраного диска.

На сторінці *Аудит* можна ввести список аудиту обраного диска (рисунок 3.27).

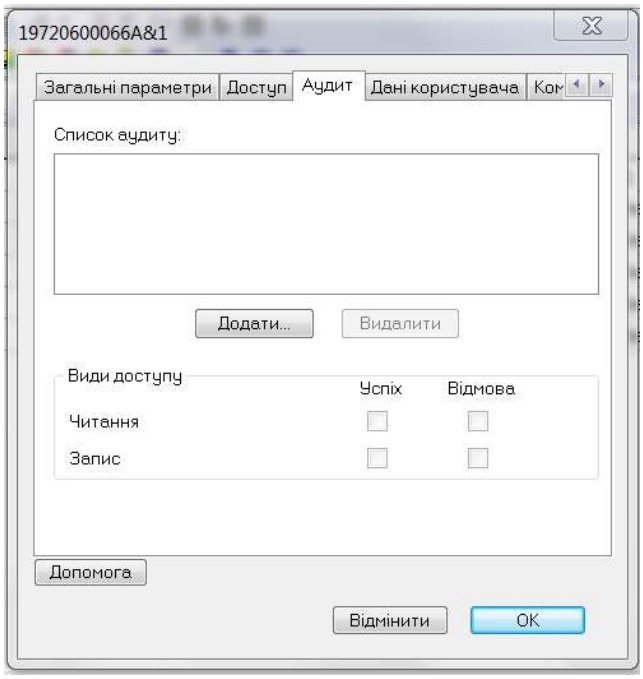

Рисунок 3.27 – Діалогове вікно для введення списку аудиту диска

За допомогою кнопки ***Додати*** можна додати користувача чи групу користувачів до списку аудиту диска. Відмітка у полі ***Успіх*** означає, що для користувача або групи користувачів буде встановлено аудит успішного доступу на читання та/або запис до цього диска, відмітка у полі ***Відмова*** означає, що буде встановлено аудит відмов у доступі на читання та/або запис до цього диска. За допомогою кнопки ***Видалити*** можна видалити користувача із списку аудиту диска.

На сторінці ***Дані користувача*** можна ввести дані, структура яких задана шаблоном користувача (рисунок 3.28). Визначення шаблону описане в п. 3.2.7.1.7.

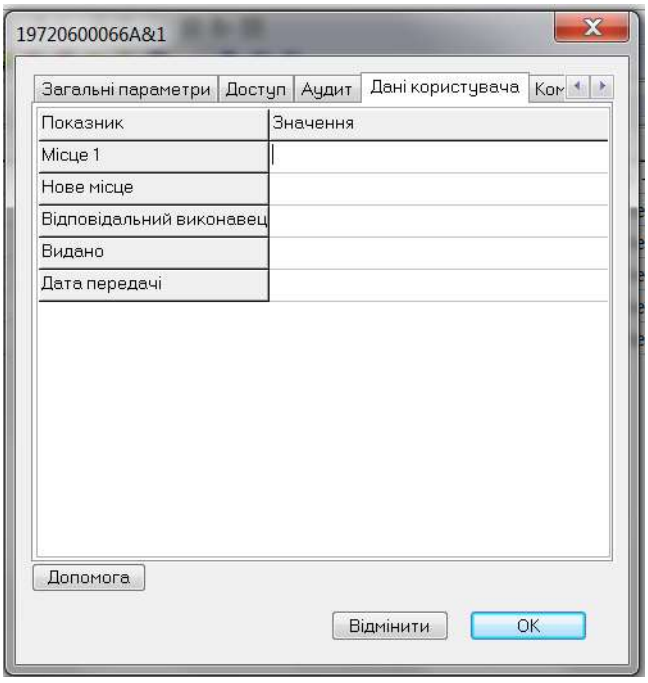

Рисунок 3.28 – Діалогове вікно для уведення даних користувача

Крім того, може бути введений довільний опис диска у полі "Коментар" (рисунок 3.29).

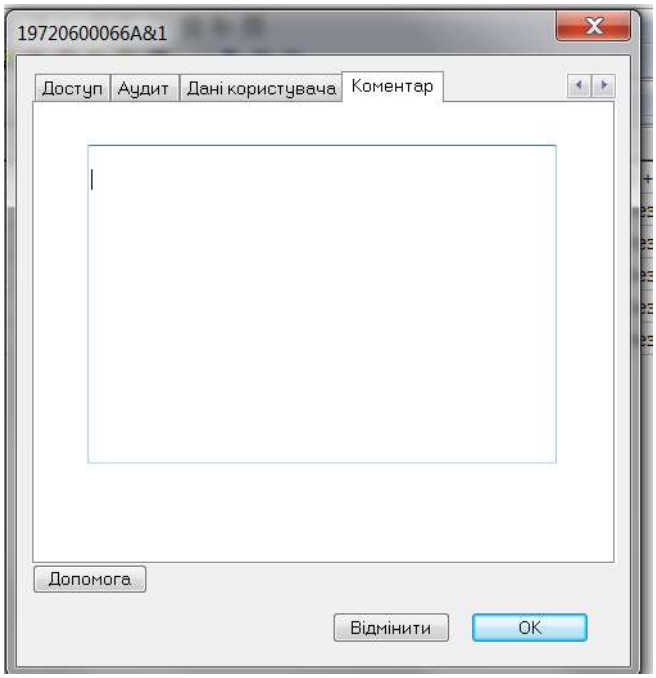

Рисунок 3.29 – Діалогове вікно для уведення довільного опису диска (колонка "Коментар")

3.2.6.2 Видалення даних про зареєстрований диск USB Flash

Для того, щоб видалити дані про зареєстрований диск USB Flash, треба вибрати відповідний рядок у переліку зареєстрованих дисків і скористатись пунктом меню *Коригування – Видалити дані про знімний диск* або натиснути кнопку . Після підтвердження дані про зареєстрований диск буде видалено.

3.2.6.3 Коригування даних про зареєстрований диск USB Flash

Для того, щоб скоригувати дані про зареєстрований диск USB Flash, треба вибрати відповідний рядок у переліку зареєстрованих дисків та скористатись пунктом меню *Коригування – Коригувати дані про знімний диск* або натиснути кнопку . Крім того, коригування поточного диску відбувається при натисканні клавіші Enter (або подвійному натискання лівої клавіші миші). Коригування відбувається за правилами, наведеними в п. 3.2.6.1.

3.2.7 Налаштування параметрів конфігурації системи

За допомогою пункту головного меню *Конфігурація* проводиться встановлення значень параметрів конфігурації, повний перелік яких наведено в Додатку А документа “Загальний опис системи”.

3.2.7.1 Встановлення загальних параметрів

3.2.7.1.1 Встановлення параметрів реєстрації подій

3.2.7.1.1.1 Встановлення параметрів журналу реєстрації

За допомогою пункту меню ***Конфігурація – Загальні параметри – Реєстрація подій – Видалення резервних копій*** або кнопки  встановлюються такі параметри конфігурації системи:

- видаляти старі звіти та копії журналу;
- максимальний вік звітів та копій журналу;
- видаляти лише архівні звіти та копії журналу.

Для встановлення параметрів журналу захисту призначено діалогове вікно ***Параметри видалення резервних копій журналу реєстрації подій*** (рисунок 3.30).

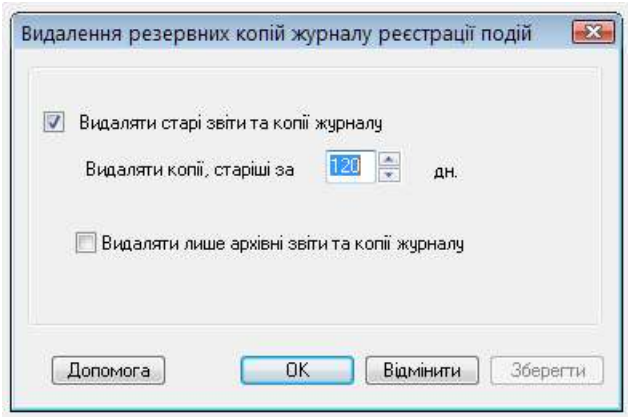

Рисунок 3.30 – Діалогове вікно для встановлення параметрів *видалення резервних копій* журналу

Відмітка в полі ***Видаляти старі звіти та копії журналу*** означає, що відбувається автоматичне видалення звітів та копій журналу реєстрації.

Відмітка в полі ***Видаляти копії, старіші за … днів*** означає, що копії, вік яких менший за вказаний, видалятись не будуть.

Відмітка в полі ***Видаляти лише архівні звіти та копії журналу*** означає, що будуть видалятись тільки ті файли, для яких не встановлено атрибут ***архівний*** (звичайно цей атрибут знімають програми резервного копіювання).

3.2.7.1.1.2 Встановлення реакції на небезпечні події

За допомогою пункту меню ***Конфігурація – Параметри комп'ютера – Реєстрація подій – Реакція на небезпечні події*** або кнопки  встановлюються такі параметри конфігурації системи:

- звукова сигналізація про небезпечні події;
- зміна стану після небезпечної події;
- створення звіту про небезпечні події.

Для формування цих параметрів призначено діалогове вікно ***Реакція на небезпечні події*** (рисунок 3.31).

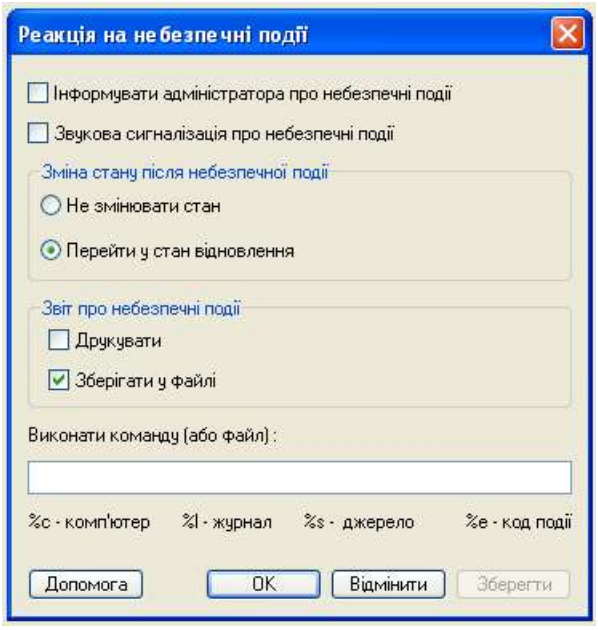

Рисунок 3.31 – Діалогове вікно для визначення реакції на небезпечні події

При встановленій відмітці в полі *Звукова сигналізація про небезпечні події* реєстрація в журналі кожної небезпечної події супроводжуватиметься звуковим сигналом.

Група полів *Зміна стану після небезпечної події* визначає, чи буде здійснено перехід системи у стан відновлення у випадку реєстрації в журналі небезпечної події.

Група полів *Звіт про небезпечні події* визначає, в якому саме вигляді буде створюватись звіт – він може бути надрукований та/або збережений у файлі.

При виникненні небезпечної події може також виконуватись вказана *команда*.

Команда являє собою будь-яку команду, що може вказуватись у Windows (наприклад, у командному рядку або в діалоговому вікні Windows *Виконати*). Це може бути файл, що виконується (.exe, .cmd, .bat і т.д.) з параметрами. Для файлу повинна також вказуватись директорія, в якій він знаходиться (якщо це не загальнодоступна директорія операційної системи). В параметрах можуть використовуватись умовні позначення, наведені на формі. Наприклад, може бути задана команда:

D:\Utilites\ShowMess.exe “Небезпека”

Можна вказувати також команди операційної системи (наприклад, Copy, Move та інші).

3.2.7.1.2 Встановлення параметрів роботи з документами

3.2.7.1.2.1 Встановлення політики документів

Політика документів встановлюється для баз документів з адміністративним та довірчим керуванням доступом. За допомогою пункту меню *Конфігурація – Загальні параметри – Робота з документами – Політика документів* або кнопки  встановлюються такі параметри конфігурації системи:

- обмеження для адміністратора документів;
- дозволяти створення довірчих баз;
- максимальний рівень доступу для довірчих баз;
- реєструвати події для довірчих баз;

– примусове маркування документів перед друком;

– мінімальний рівень доступу для примусового маркування документів;

– запитувати обліковий номер документа перед друком;

– мінімальний рівень доступу, для якого запитується обліковий номер документа перед друком.

Для встановлення цих параметрів призначене Діалогове вікно ***Політика документів*** (рисунок 3.32).

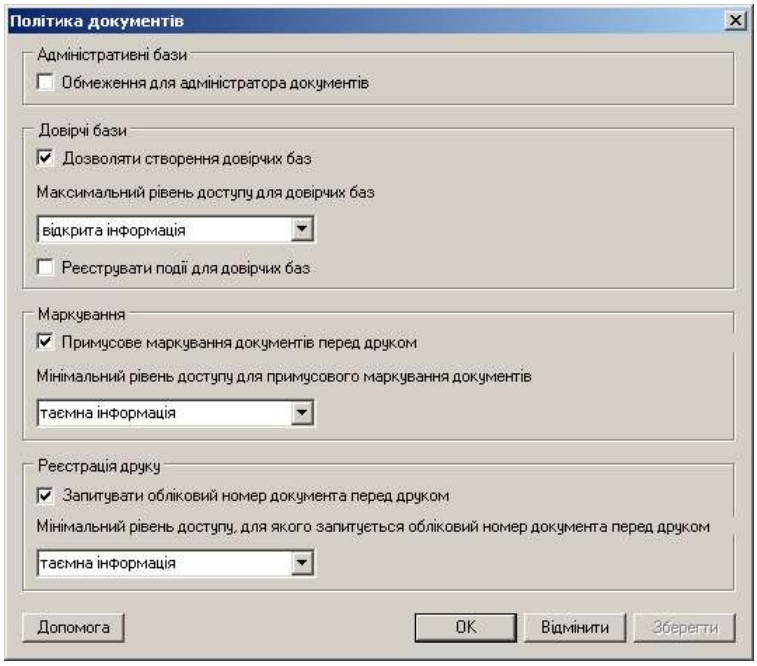

Рисунок 3.32 – Діалогове вікно для встановлення політики документів

Відмітка в полі ***Обмеження для адміністратора документів*** означає, що користувачу з роллю ***Адміністратор документів*** під час роботи з базами документів з адміністративним керуванням доступом не надаються дозволи на такі види доступу:

доступ до баз документів:

– створення документів;

доступ до документів:

– запис вмісту документа;
– запис стандартних та додаткових атрибутів;
– видалення;
– друк;
– експорт.

Відмітка в полі ***Дозволяти створення довірчих баз*** означає, що в системі дозволяється створювати бази з довірчим керуванням доступом.

У полі ***Максимальний рівень доступу для довірчих баз*** встановлюється максимальний рівень доступу документів, які можуть міститись в базах із довірчим керуванням доступом.

Відмітка в полі ***Реєстрація подій для довірчих баз*** означає, що для баз із довірчим керуванням доступом здійснюватиметься реєстрація подій.

Відмітка в полі *Примусове маркування документів перед друком* означає, що користувач під час друку та експорту документів, які містять інформацію з обмеженим доступом, буде змушений вказувати такі реквізити документа як гриф, літер, обліковий номер тощо.

У полі *Мінімальний рівень доступу для примусового маркування документів* встановлюється мінімальний рівень доступу документів, перед друком яких буде здійснюватись примусове маркування.

Відмітка в полі *Запитувати обліковий номер документа перед друком* означає, що перед друком буде запитуватись обліковий номер документа.

У полі *Мінімальний рівень доступу, для якого запитується обліковий номер документа перед друком* встановлюється мінімальний рівень доступу документів, перед друком яких буде запитуватись обліковий номер документа.

3.2.7.1.2.2 Встановлення попередження при вході в базу документів

За допомогою пункту меню *Конфігурація – Загальні параметри – Робота з документами – Попередження при вході в базу документів* або кнопки  встановлюються такі параметри конфігурації системи:

– текст попередження при вході в базу документів з рівнем доступу таємно або вищим;

– виводити попередження при вході в базу документів з рівнем доступу таємно або вищим.

Ці параметри передбачені тільки для конфігурації "Підвищена безпека".

Попередження призначене для нагадування користувачеві про те, що він працює з документами обмеженого доступу та має дотримуватись певних правил. Попередження виводиться після того, як користувач перший раз за сеанс роботи з програмою "Захищені документи" входить у базу документів з рівнем доступу таємно або вищим. Виведення цього попередження можна відключити. За умовчанням передбачено виводити це попередження.

3.2.7.1.3 Встановлення доступу до технологічної інформації

За допомогою пункту меню *Конфігурація – Загальні параметри – Доступ до технологічної інформації* або кнопки  встановлюється параметр конфігурації системи дозволи на доступ до технологічної інформації.

Для встановлення цього параметра призначене діалогове вікно *Доступ до технологічної інформації* (рисунок 3.33).

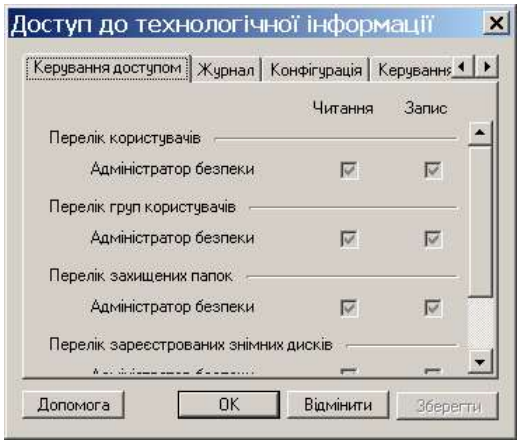

Рисунок 3.33 – Діалогове вікно для встановлення доступів до технологічної інформації

На кожній сторінці встановлюються доступи адміністраторів до окремих складових даних захисту:

– бази облікових записів та даних про об’єкти захисту;
– журналу реєстрації;
– параметрів конфігурації системи;
– оперативних даних про роботу системи.

До кожної зі складових даних захисту встановлюються дозволи на читання та запис. Частина дозволів не може бути змінена (у цьому випадку відмітка стоїть на сірому фоні).

3.2.7.1.4 Встановлення політики паролів

За допомогою пункту меню *Конфігурація – Загальні параметри – Політика облікових записів – Політика паролів* або кнопки  встановлюються такі параметри конфігурації системи:

– паролі повинні задовольняти вимогам щодо складності;
– мінімальна довжина пароля;
– мінімальний термін дії пароля;
– максимальний термін дії пароля;
– кількість неповторюваних паролів.

Для встановлення цих параметрів призначене діалогове вікно *Політика паролів* (рисунок 3.34).

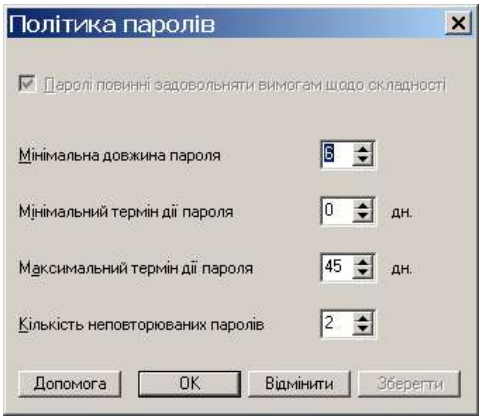

Рисунок 3.34 – Діалогове вікно для встановлення політики паролів

Відмітка в полі *Паролі повинні відповідати вимогам складності* змушує користувача використовувати досить складні паролі.

Значення поля *Мінімальна довжина пароля* визначає мінімальну довжину пароля, який вводитиме користувач.

Значення поля *Мінімальний термін дії пароля* не дозволяє користувачу змінити пароль, якщо він вже був щойно змінений і таким чином, після декількох змін повернутись до старого пароля.

Значення поля *Максимальний термін дії пароля* визначає термін, після закінчення якого система змушує користувача змінювати пароль.

Значення параметра *Кількість неповторюваних паролів* обмежує можливість користувача використовувати старі паролі під час зміни пароля.

3.2.7.1.5 Встановлення політики блокування облікового запису

За допомогою пункту меню *Конфігурація – Загальні параметри – Політика облікових записів – Політика блокування облікового запису* або кнопки встановлюються такі параметри конфігурації системи:

– максимальна кількість невдалих спроб входу до системи;

– інтервал для поновлення відліку невдалих спроб входу до системи.

Для встановлення цих параметрів призначене діалогове вікно *Політика блокування облікового запису* (рисунок 3.35).

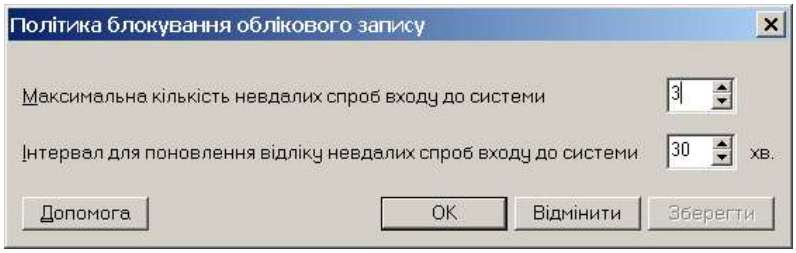

Рисунок 3.35 – Діалогове вікно для встановлення політики блокування облікового запису

У полі *Максимальна кількість невдалих спроб входу до системи* вказується кількість невдалих спроб входу до системи, після яких обліковий запис блокується.

У полі *Інтервал для поновлення відліку невдалих спроб входу до системи* вказується інтервал, після закінчення якого відлік невдалих спроб входу поновлюється.

3.2.7.1.6 Встановлення параметрів, пов'язаних із входом до системи

3.2.7.1.6.1 Встановлення параметрів входу до системи

За допомогою пункту меню *Конфігурація – Загальні параметри – Вхід до системи – Параметри входу до системи* або кнопки  встановлюються такі параметри конфігурації системи:

– `перевіряти ключовий диск під час входу до Windows;`

– `перевіряти ключовий диск під час роботи у Windows;`

– `відображати ім'я попереднього користувача;`

– `дозволяти швидке переключення користувачів.`

Для встановлення цих параметрів призначене діалогове вікно *Вхід до системи* (рисунок 3.36).

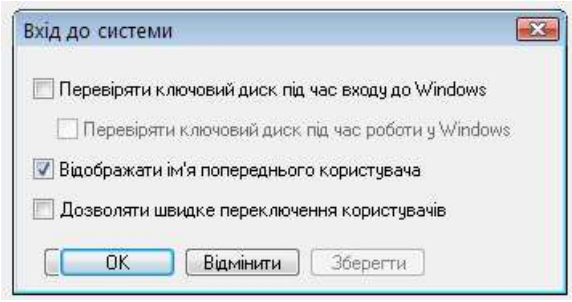

Рисунок 3.36 – Діалогове вікно для встановлення параметрів входу до системи

Усі наведені параметри можуть приймати значення *Так* та *Ні*.

Значення *Так* параметра конфігурації `перевіряти ключовий диск під час входу до Windows` означає, що увійти до системи та розблокувати комп'ютер можуть тільки ті користувачі, які мають обліковий запис у системі ЛОЗА-1 та, за необхідності, ключовий диск.

Якщо параметр `перевіряти ключовий диск під час роботи у Windows` має значення *Так*, у випадку видалення ключового диска під час роботи комп'ютер автоматично блокується. Значення параметра може бути встановлене тільки у тому випадку, коли для параметра `перевіряти ключовий диск під час входу до Windows` задано значення *Так*.

Параметр `відображати ім'я попереднього користувача` впливає на екран входу до системи. Для Windows 7/8.1/10/2012/2016/2019 цей параметр визначає, чи відображається на екрані перелік користувачів системи.

3.2.7.1.6.2 Визначення попередження при вході до системи

За допомогою пункту меню *Конфігурація – Загальні параметри – Вхід до системи – Попередження при вході до системи* або кнопки  встановлюються такі параметри конфігурації системи:

– текст попередження при вході до системи;
– виводити попередження при вході до системи.

Для встановлення цих параметрів призначено діалогове вікно ***Попередження при вході до системи*** (рисунок 3.37).

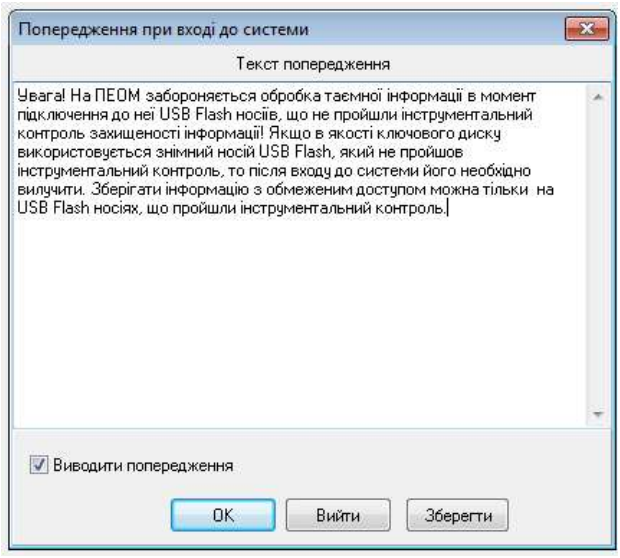

Рисунок 3.37 – Діалогове вікно для встановлення попередження при вході до системи

Попередження призначене для нагадування користувачеві про те, що він працює з інформацією обмеженого доступу та має дотримуватись певних правил. Попередження виводиться після того, як користувач пройшов ідентифікацію та автентифікацію і починає роботу в системі. Виведення цього попередження можна відключити. За умовчанням передбачено виводити це попередження для конфігурації "Підвищена безпека", та не виводити для конфігурації "Стандартна безпека".

Приклад видачі такого попередження для операційної системи Windows 7 наведено далі.

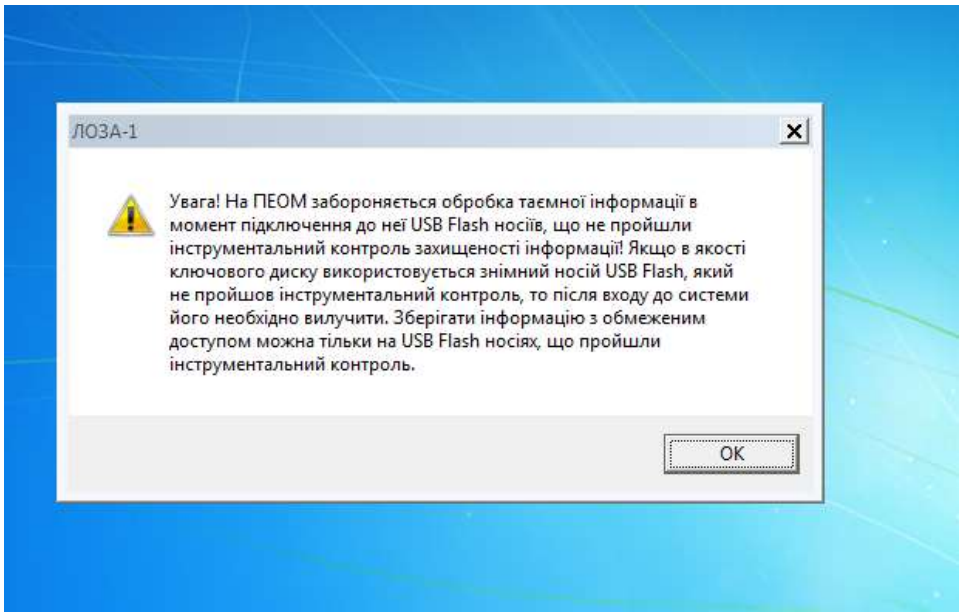

Рисунок 3.38 – Попередження при вході до системи

3.2.7.1.7 Визначення шаблонів користувача для зареєстрованих дисків USB Flash

За допомогою пункту меню *Конфігурація – Загальні параметри – Шаблони користувача - Зареєстровані диски USB Flash* або кнопки  користувач може визначити власні шаблони для опису зареєстрованих дисків USB Flash за допомогою ділового вікна (рисунок 3.39).

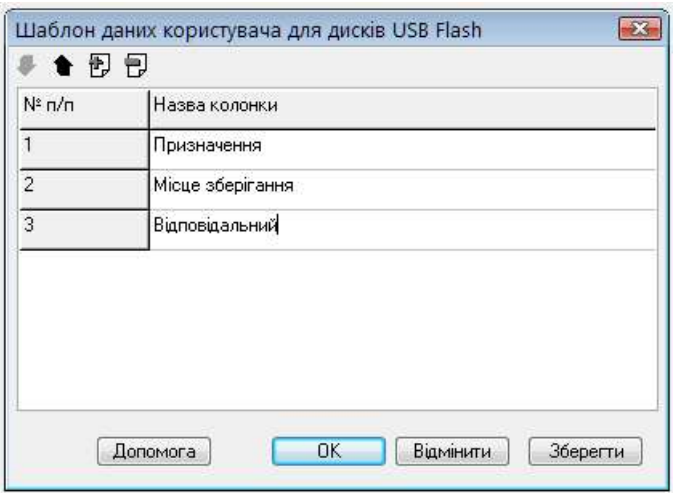

Рисунок 3.39 – Діалогове вікно для визначення шаблонів користувача для опису зареєстрованих дисків USB Flash

За допомогою кнопок "Додати" та "Видалити" додаються/видаляються поля опису. За допомогою стрілок вверх або вниз можна змінювати порядок колонок опису. Слід пам’ятати, що потрібно бути уважним при коригуванні раніше створених шаблонів. Якщо потрібно змінити призначення колонки, то стару колонку потрібно видалити, а нову додати, інакше нова колонка успадкує вміст від старої.

Цей шаблон відображається при перегляді та коригуванні списку зареєстрованих дисків USB Flash. Якщо користувач визначив шаблон так, як зображено (рисунок 3.39), то при перегляді списку дисків він матиме список колонок (рисунок 3.40).

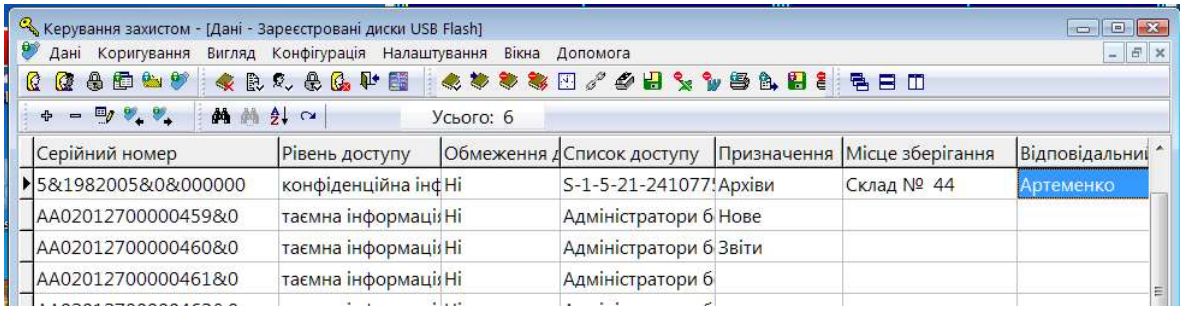

Рисунок 3.40 – Діалогове вікно для перегляду зареєстрованих дисків USB Flash з шаблоном, визначеним користувачем

3.2.7.1.8 Встановлення параметрів безпечного видалення інформації

Для прискорення роботи системи із захищеними папками та зареєстрованими дисками USB Flash передбачено параметр, який визначає рівень секретності, починаючи з якого потрібно проводити безпечне видалення інформації (за допомогою процедури Wipe). Це видалення займає певний час, але після нього відновлення інформації неможливе. На рисунку показане діалогове вікно для встановлення параметру (

рисунок 3.41). При такому визначенні параметра, як вказано на рисунку, вся інформація з рівнем "Конфіденційна" та вищим буде видалятися із захищених папок та дисків USB Flash за допомогою процедури Wipe (тобто безпечно). Рівень секретності стосується папки або диска USB Flash в цілому, а не окремих файлів та папок, що містяться в них.

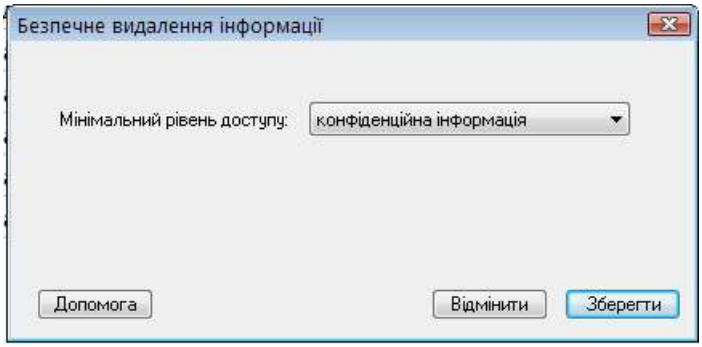

Рисунок 3.41 – Діалогове вікно для визначення мінімального рівня безпечного видалення інформації

3.2.7.2 Встановлення параметрів комп'ютера

3.2.7.2.1 Встановлення параметрів реєстрації подій

3.2.7.2.1.1 Встановлення параметрів журналу реєстрації подій

В цьому пункті головного меню визначаються такі параметри конфігурації:

– граничний розмір журналу системи ЛОЗА-1;
– команда, що виконується при створенні резервної копії журналу.

Діалогове вікно, за допомогою якого відбувається настройка цих параметрів, наведене далі (рисунок 3.42).

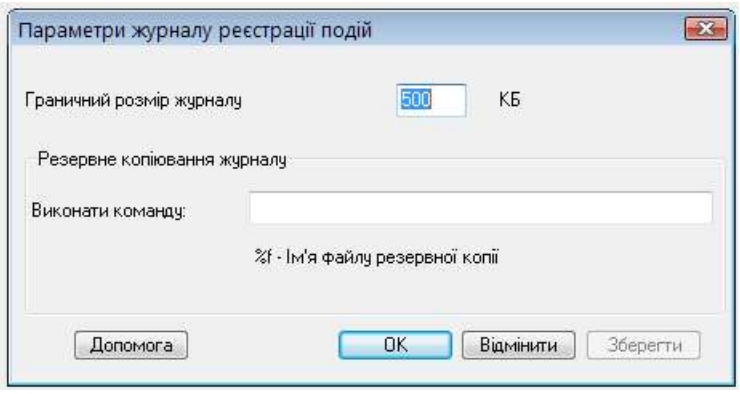

Рисунок 3.42 – Діалогове вікно для визначення параметрів журналу реєстрації подій

3.2.7.2.1.2 Встановлення політики аудиту

Політика аудиту системи визначається параметром конфігурації системи `політика аудиту`.

Політика аудиту системи встановлюється для таких категорій подій джерела *LOZAAudit*:

– ***вхід/вихід*** (вхід користувачів до системи, зміна пароля користувача, вихід із системи та ін.);

– ***робота з програмами*** (запуск та завершення роботи прикладних програм системи);

– ***керування доступом*** (коригування бази облікових записів та даних про об'єкти захисту);

– ***конфігурація*** (читання та зміна значень параметрів конфігурації системи);

– ***керування системою*** (зміна стану системи, визначення початкового стану для наступного сеансу роботи та ін.);

Встановлюється політика аудиту за допомогою пункту меню ***Конфігурація – Параметри комп'ютера – Реєстрація подій – Політика аудиту*** або кнопки  . Для встановлення політики аудиту призначене діалогове вікно ***Політика аудиту*** (рисунок 3.43).

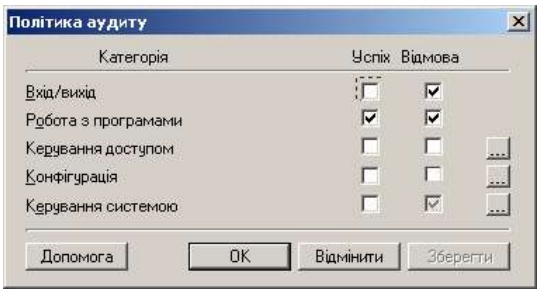

Рисунок 3.43 – Діалогове вікно для налаштування політики аудиту

Аудит може бути встановлений окремо для різних видів доступу, а також для успішних та невдалих спроб доступу. Для параметрів конфігурації аудит може бути встановлений для різних груп параметрів.

3.2.7.2.1.3 Встановлення параметрів імпорту подій

За допомогою пункту меню ***Конфігурація – Параметри комп'ютера – Реєстрація подій – Імпорт подій*** або кнопки  встановлюються такі параметри конфігурації системи:

– перелік подій, які імпортуються до журналу захисту;

– імпортувати всі помилки.

Для встановлення цих параметрів призначено діалогове вікно ***Імпорт подій*** (рисунок 3.44).

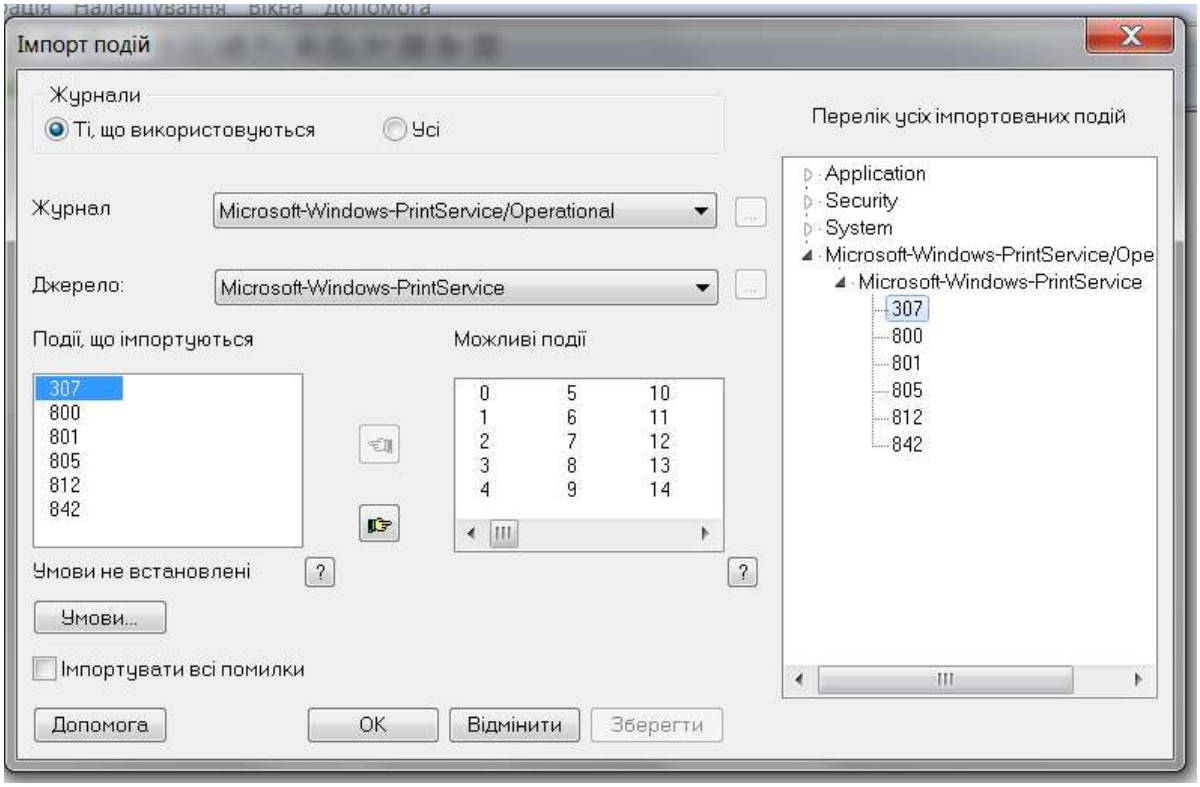

Рисунок 3.44 – Діалогове вікно для встановлення параметрів імпорту подій

Імпорт подій відбувається із трьох журналів Windows – *Журнала приложений, Журнала безопасности* та *Системного журнала*, а для Windows 7 та вищих версій – також з журналів *Приложений и служб (Applications and services Logs)*. Для вибору за допомогою спеціальної настройки можна брати журнали:

- ті, що використовуються:
- усі можливі для аналізу.

Якщо вибрано усі можливі журнали, то переглянути їх список можна не тільки у списку, що випадає, але й за допомогою спеціальної форми (рисунок 3.45), де передбачено контекстний пошук. Аналогічна форма передбачена для пошуку джерела для тих журналів, які містять 10 або більше джерел подій.

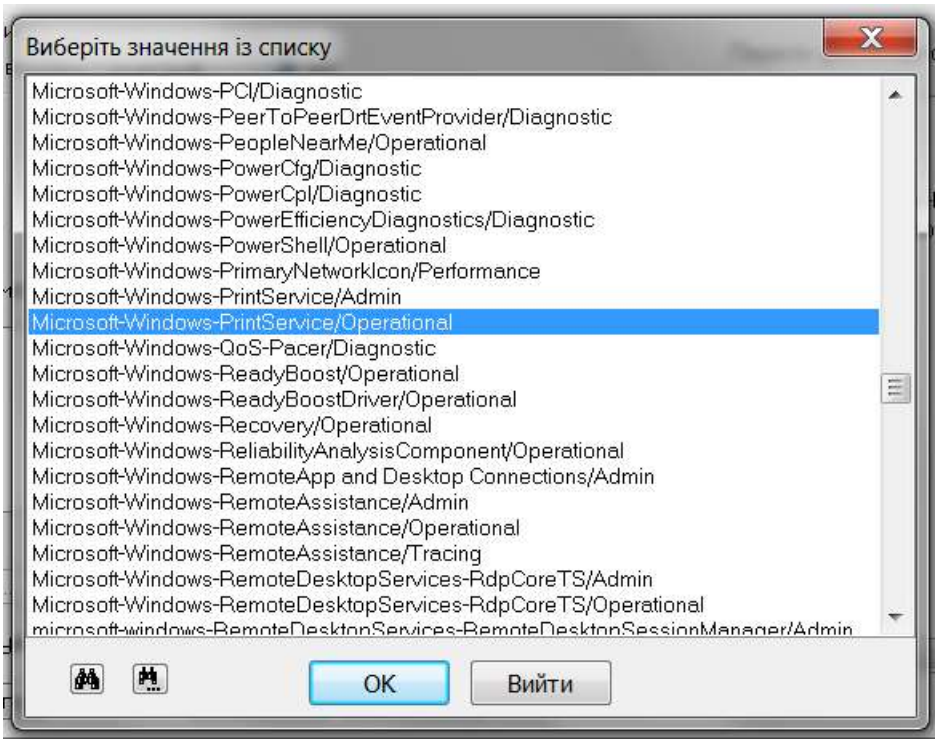

Рисунок 3.45 – Діалогове вікно для пошуку журналу

Після вибору одного з журналів Windows необхідно вибрати джерело подій із переліку джерел, що відповідають вибраному журналу. При цьому відображаються два списки подій:

– події, що імпортуються, тобто події, які вже включено до переліку подій, що імпортуються;

– можливі події, тобто події, які ще можна включити до переліку подій, що імпортуються.

Для кожного з журналів ***Приложений и служб*** передбачено лише одне джерело. Воно вибирається автоматично. Слід зазначити, що саме в цій групі журналів знаходяться події, пов'язані з друком для версій Windows 7 та вищих, а саме у журналі, відміченому на рисунку (рисунок 3.45). Шаблони опису деяких з цих подій наведено на рисунку (рисунок 3.46). За умовчанням у список подій, що імпортуються, включено подію з кодом 307, тобто власне друк. Для того, щоб подія друку імпортувалась до журналу системи ЛОЗА, потрібно забезпечити ведення відповідного журналу в операційній системі (див. п.2.2 документа ***Інструкція системного адміністратора***). Слід зазначити, що для аудиту друку документів через програму ***Захищені документи*** передбачена спеціальна подія в джерелі ***LozaAudit*** (код 58004).

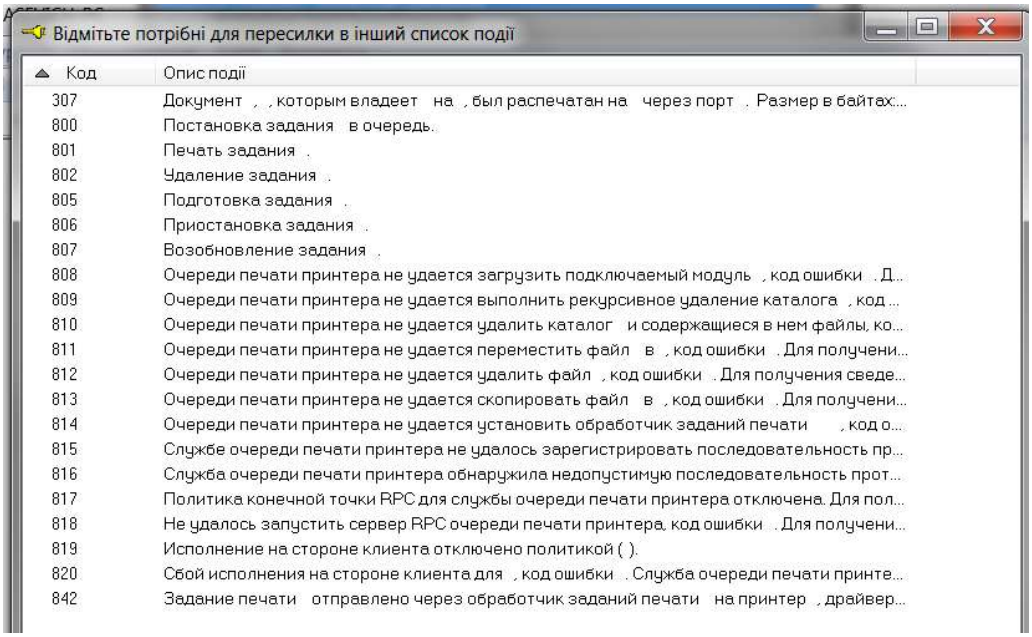

Рисунок 3.46 – Шаблони опису подій, пов’язаних з друком

В правій частині форми наведено (у вигляді дерева) перелік подій, що вже визначені у системі як імпортовані. При подвійному натисканні на елемент (джерело або код події) він відмічається у лівій частині форми. Для спрощення роботи з кодами подій передбачено кнопки [?] під списками подій. При натисканні на одну з цих кнопок виводиться розшифровка кодів подій – для них виводиться початок шаблону опису. Приклад такого списку наведено далі (рисунок 3.47). У ньому можно проводити пошук та відмічати потрібні події. Ця відмітка збережеться при поверненні на основну форму.

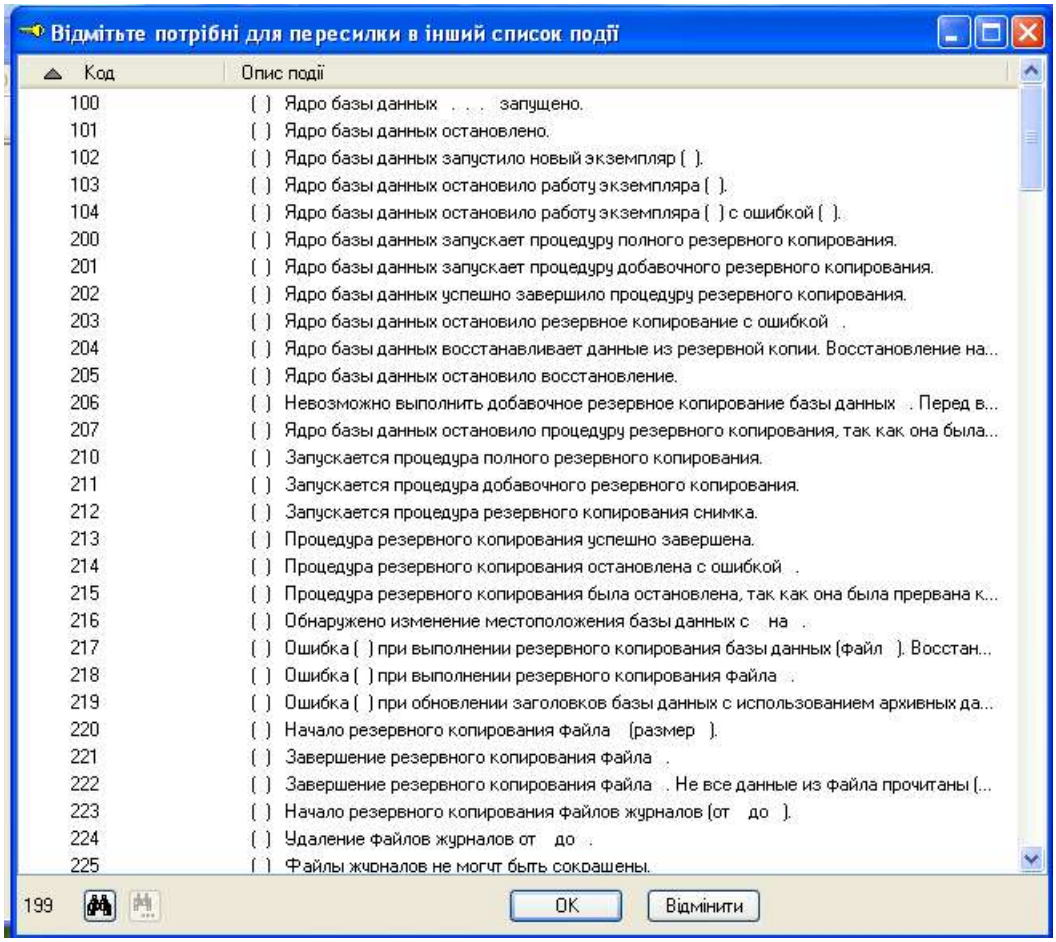

Рисунок 3.47 – Діалогове вікно з переліком кодів та шаблонів подій для вибраного журналу та джерела

За допомогою кнопок та до переліку подій, що імпортуються, можна включати додаткові події зі списку можливих подій, а також видаляти з нього події, якщо включення їх до журналу захисту стало непотрібним.

При встановленій відмітці в полі *Імпортувати всі помилки* всі події з журналів Windows, які мають тип *Помилка*, імпортуватимуться до журналу захисту (незалежно від того, чи зазначені вони в першому параметрі).

За допомогою кнопки *Умови* для вибраної події може бути задана довільна кількість умов імпорту. Якщо справджується хоча б одна із заданих умов, подія імпортується.

Для встановлення умов імпорту призначено діалогове вікно *Умови для події* (рисунок 3.48).

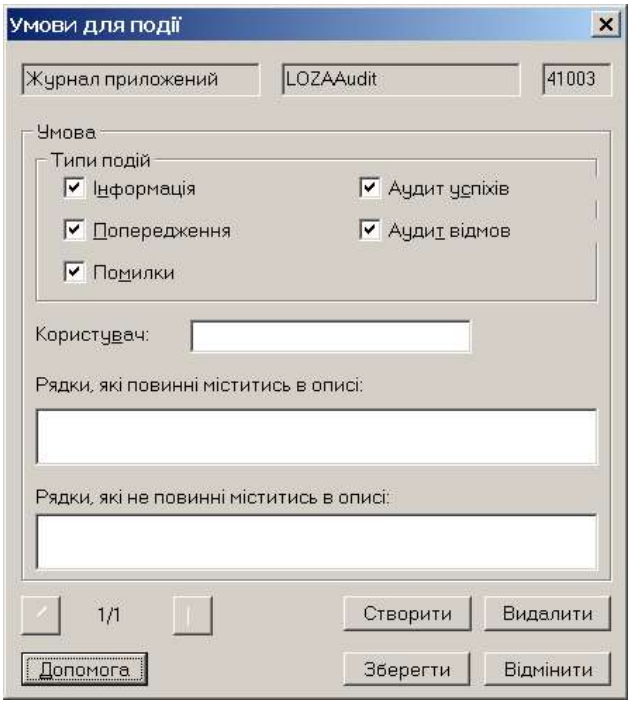

Рисунок 3.48 – Діалогове вікно для встановлення умов для імпорту події

Кожна умова може містити такі елементи:

– тип події;
– ім’я користувача, від імені якого подія була зареєстрована;
– перелік рядків, кожний з яких повинен міститись в описі події;
– перелік рядків, кожний з яких не повинен міститись в описі події.

Щоб уникнути помилок, фрагменти рядків, які повинні (або не повинні) міститися в описі, краще копіювати безпосередньо з журналів Windows. Ці фрагменти можуть включати в себе спеціальні символи, які не відображаються при перегляді.

За допомогою кнопки ***Створити*** можна додати нову умову, за допомогою кнопки ***Видалити*** – видалити одну умову.

3.2.7.2.1.4 Визначення небезпечних подій

За допомогою пункту меню ***Конфігурація – Параметри комп’ютера – Реєстрація подій – Небезпечні події*** або кнопки встановлюються такі параметри конфігурації системи:

– `перелік небезпечних подій`;
– `вважати помилки небезпечними подіями`.

Для встановлення цих параметрів призначено діалогове вікно ***Небезпечні події*** (рисунок 3.49).

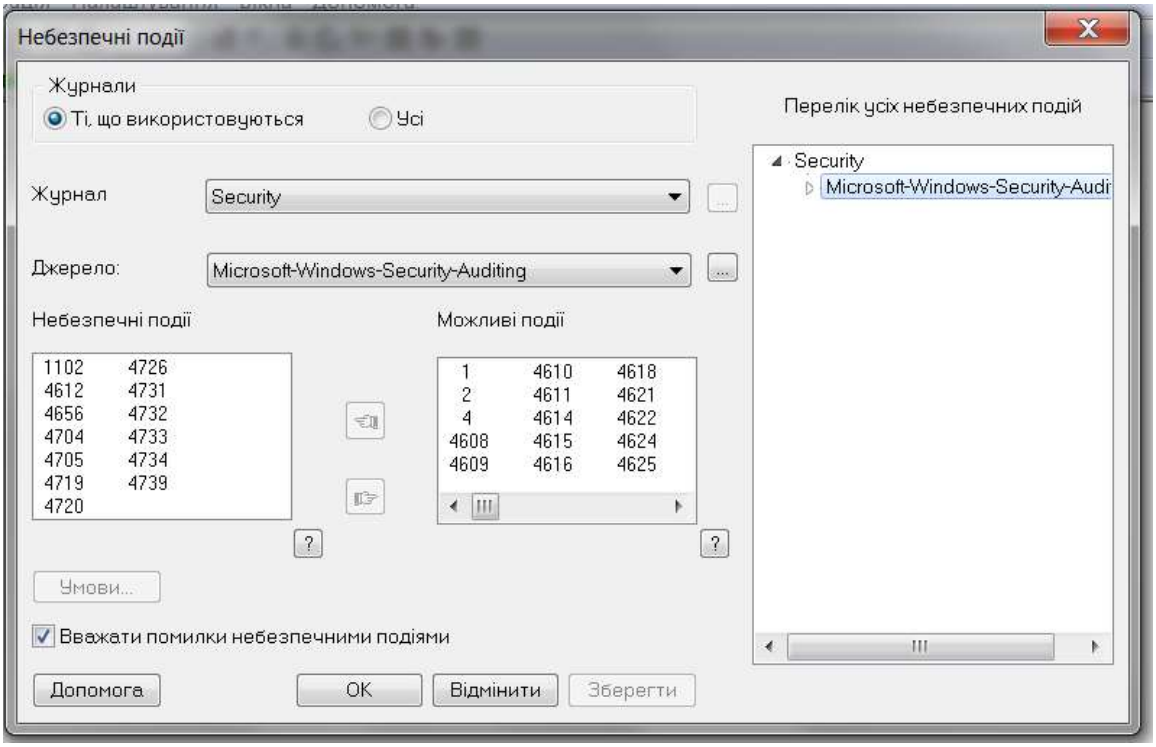

Рисунок 3.49 – Діалогове вікно для визначення небезпечних подій

Робота з переліком небезпечних подій аналогічна роботі з переліком імпортованих подій (п. 3.2.7.2.1.3) за виключенням того, що при виборі *Усі* для журналів в перелік включаються тільки ті, що є в переліку подій для імпорту.

При встановленій відмітці в полі *Вважати помилки небезпечними подіями,* всі події, зареєстровані в журналі захисту під час роботи системи, які мають тип *Помилка*, вважатимуться небезпечними (незалежно від того, чи зазначені вони в першому параметрі).

За допомогою кнопки *Умови* для вибраної події може бути задана довільна кількість умов, за яких подія буде вважатись небезпечною. Якщо справджується хоча б одна із заданих умов, подія вважається небезпечною.

3.2.7.2.2 Встановлення додаткових засобів адміністрування

За допомогою пункту меню *Конфігурація – Загальні параметри – Додаткові засоби адміністрування* або кнопки  встановлюються додаткові параметри адміністрування системи.

Це такі параметри конфігурації системи:

– `команда для сигналізації про зміну стану` – команда, яка виконується одразу після того, як система змінює стан; команда приймає такі параметри:

- %c – код стану;
- %n – назва стану;

– `команда для сигналізації про помилку під час виконання операції` – команда, яка виконується одразу після того, як виникає помилка під час виконання операції; команда приймає такі параметри:

- %c – код операції;
- %n – назва операції;
- %m – повідомлення про помилку.

Діалогове вікно для визначення цих параметрів наведене далі (рисунок 3.50).

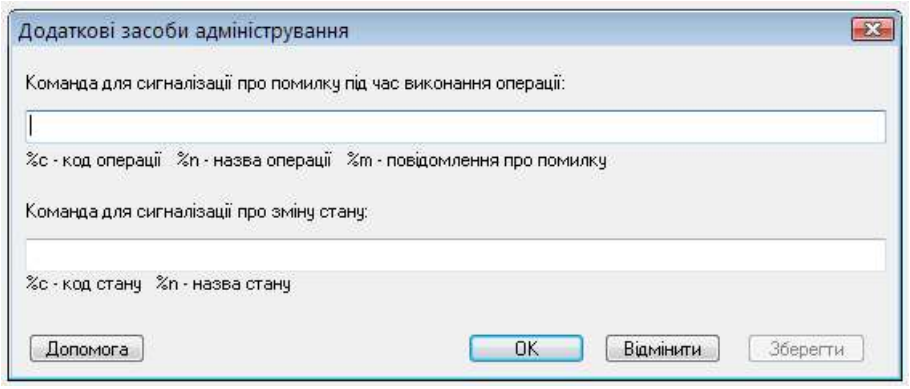

Рисунок 3.50 – Діалогове вікно для встановлення додаткових засобів адміністрування

3.2.7.2.3 Встановлення параметрів перевірки цілісності

Параметри перевірки цілісності встановлюються за допомогою пункту меню *Конфігурація – Параметри комп'ютера – Перевірка цілісності* або кнопки .

3.2.7.2.3.1 Загальні параметри

До загальних параметрів перевірки цілісності відносяться такі параметри:

- реакція на порушення цілісності;
- об'єкти для перевірки цілісності;
- періодичність перевірки цілісності.

Для встановлення загальних параметрів перевірки цілісності призначено сторінку *Загальні параметри* діалогового вікна *Параметри перевірки цілісності* (рисунок 3.51).

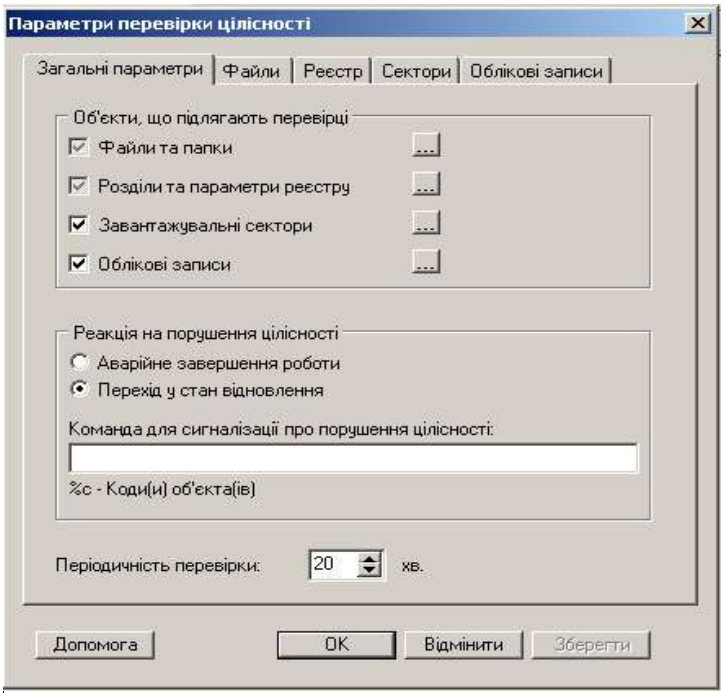

Рисунок 3.51 – Діалогове вікно для встановлення загальних параметрів перевірки цілісності

У групі *Об'єкти, що підлягають перевірці* визначається, що саме перевіряється. На цілісність можуть перевірятись такі об'єкти:

– файли та папки;
– розділи та параметри системного реєстру;
– завантажувальні сектори жорстких дисків комп'ютера;
– облікові записи.

Для кожного виду об'єктів за допомогою кнопки ... встановлюється режим перевірки. Перевірки можуть виконуватись:

– на початку роботи;
– періодично;
– постійно під час роботи (тільки файли та папки і розділи та параметри реєстру).

Перевірка на початку роботи є обов'язковою, якщо встановлена періодична або постійна перевірка.

У групі *Реакція на порушення цілісності* визначається, як система реагує на порушення цілісності: аварійно завершує роботу чи переходить у стан відновлення.

У полі *Періодичність перевірки* вводиться інтервал (у хвилинах) між автоматичними перевірками цілісності.

3.2.7.2.3.2 Перевірка цілісності файлів та папок

3.2.7.2.3.2.1 Основні параметри

Перевірці підлягають усі файли вказаних типів, які містяться у вказаних папках, при цьому враховуються окремі файли, що підлягають та не підлягають перевірці, та папки, що не підлягають перевірці. Якщо перелік папок не вказано, перевіряються всі файли вказаних типів на всіх жорстких дисках.

До основних параметрів перевірки цілісності файлів та папок відносяться такі параметри:

– перелік типів файлів для перевірки цілісності;
– перелік папок для перевірки цілісності;
– ім'я файлу звіту про перевірку цілісності файлів та папок;
– граничний розмір файлу звіту про перевірку цілісності файлів та папок.

Для встановлення основних параметрів перевірки цілісності файлів та папок призначено сторінку *Файли* діалогового вікна *Параметри перевірки цілісності* (рисунок 3.52).

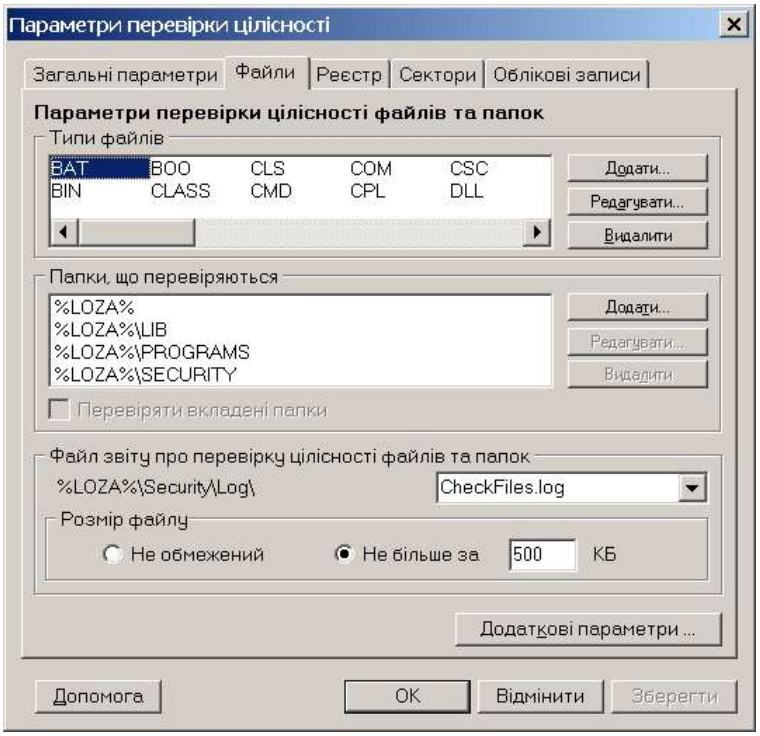

Рисунок 3.52 – Діалогове вікно для встановлення основних параметрів перевірки цілісності файлів та папок

За допомогою кнопки ***Додаткові параметри*** встановлюються додаткові параметри перевірки цілісності файлів та папок.

3.2.7.2.3.2.1.1 Встановлення переліку типів файлів, що підлягають перевірці

Тип файлу визначається за його розширенням. Кожний тип файлів може бути включений до переліку тільки один раз.

Кнопка ***Додати*** дозволяє додати тип файлів, які буде включено до переліку типів файлів, що підлягають перевірці на цілісність. Після натискання цієї кнопки на екрані з'являється діалогове вікно ***Додати тип файлів*** для введення нового типу файлів (рисунок 3.53).

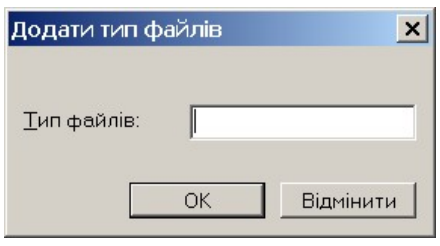

Рисунок 3.53 – Діалогове вікно для введення нового типу файлів до переліку типів файлів

Кнопка ***Редагувати*** дозволяє редагувати вибраний тип файлів. Після натискання цієї кнопки на екрані з'являється діалогове вікно ***Редагувати тип файлів*** (аналогічне вікну ***Додати тип файлів***) з ім'ям вибраного файлу, де можна провести редагування.

Кнопка ***Видалити*** дозволяє видалити зі списку вибраний тип файлів після підтвердження.

3.2.7.2.3.2.1.2 Встановлення переліку папок, що підлягають перевірці

Кнопка ***Додати*** дозволяє додати папку до переліку папок, які підлягають перевірці на цілісність.

Кнопка ***Редагувати*** дозволяє редагувати ім'я вибраної папки.

Нова папка не повинна входити до папок, які вже містяться в переліку, містити або повторювати введену папку.

Кнопка ***Видалити*** дозволяє видалити вибрану папку з відповідного переліку після підтвердження.

Відмітка в полі ***Перевіряти вкладені папки*** означає, що для цієї папки буде здійснюватись перевірка вкладених папок, – у протилежному випадку перевірятимуться лише такі об'єкти:

– сама папка – на видалення та зміни дескриптора безпеки;

– файли, що в ній знаходяться, – на зміни, видалення, створення та зміни дескрипторів безпеки;

– вкладені папки першого рівня (без файлів, які в них знаходяться) – на видалення, створення та зміни дескрипторів безпеки.

Для введення нової папки призначене діалогове вікно ***Додати папку*** (рисунок 3.54).

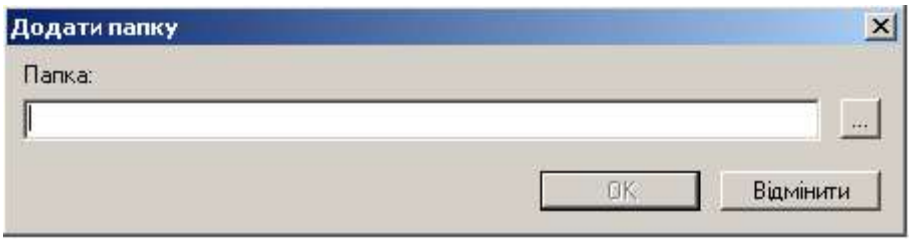

Рисунок 3.54 – Діалогове вікно для введення нової папки

У полі ***Папка*** цього вікна можна ввести ім'я нової папки вручну або вибрати її за допомогою кнопки ***Додати***.

Для редагування імені папки призначене діалогове вікно ***Редагувати папку*** (рисунок 3.55).

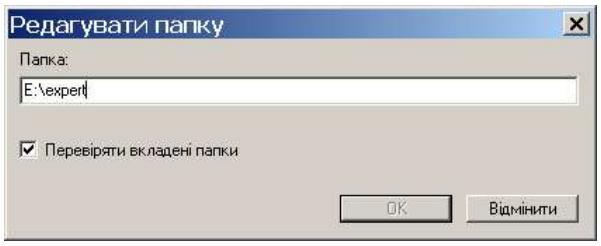

Рисунок 3.55 – Діалогове вікно для редагування імені папки

3.2.7.2.3.2.1.3 Встановлення інших параметрів

У групі ***Файл звіту про перевірку цілісності файлів та папок*** вводиться ім'я файлу, у який будуть записуватись результати перевірки цілісності файлів та папок, та його граничний розмір (в КБ).

Ім'я можна ввести ручним способом або вибрати зі списку, що випадає.

У групі ***Розмір файлу*** можна встановити обмеження на розмір файлу звіту.

3.2.7.2.3.2.2 Додаткові параметри

До додаткових параметрів перевірки цілісності файлів та папок відносяться такі параметри:

– перелік папок, для яких не здійснюється перевірка цілісності;

– перелік файлів для перевірки цілісності;

– перелік файлів, для яких не здійснюється перевірка цілісності.

Для встановлення додаткових параметрів перевірки цілісності файлів та папок призначене діалогове вікно ***Додаткові параметри,*** яке з'являється при натисканні кнопки ***Додаткові параметри*** на сторінці ***Файли*** діалогового вікна ***Параметри перевірки цілісності*** (рисунок 3.56).

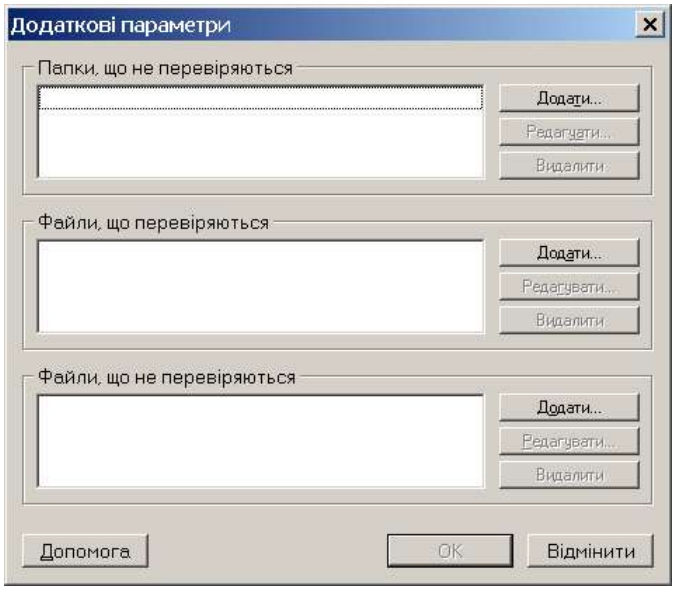

Рисунок 3.56 – Діалогове вікно для встановлення додаткових параметрів перевірки цілісності файлів та папок

3.2.7.2.3.2.2.1 Встановлення переліку папок, що не підлягають перевірці

Встановлення переліку папок відбувається за правилами, описаними в п. 3.2.7.2.3.2.1.2.

3.2.7.2.3.2.2.2 Встановлення переліку файлів, що підлягають та не підлягають перевірці

Кнопки ***Додати*** дозволяють додати ім'я файлу до відповідного переліку.

Кнопки ***Редагувати*** дозволяють редагувати ім'я вибраного файлу.

Після натискання цих кнопок з'являється стандартний діалог Windows для вибору файлу.

Кнопки ***Видалити*** дозволяють видалити ім'я вибраного файлу з відповідного переліку після підтвердження.

3.2.7.2.3.3 Перевірка цілісності розділів та параметрів реєстру

3.2.7.2.3.3.1 Основні параметри

До основних параметрів перевірки цілісності розділів та параметрів реєстру відносяться такі параметри:

– перелік розділів реєстру для перевірки цілісності;

– ім’я файлу звіту про перевірку цілісності розділів та параметрів реєстру;

– граничний розмір файлу звіту про перевірку цілісності розділів та параметрів реєстру.

Для встановлення основних параметрів перевірки цілісності розділів та параметрів реєстру призначено сторінку ***Реєстр*** діалогового вікна ***Параметри перевірки цілісності*** (рисунок 3.57).

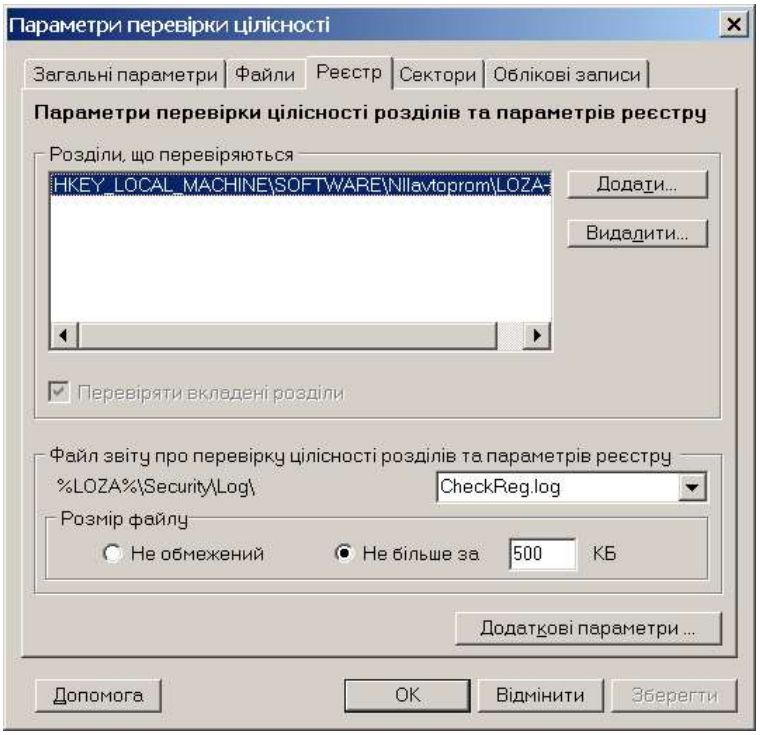

Рисунок 3.57 – Діалогове вікно для встановлення основних параметрів перевірки цілісності розділів та параметрів реєстру

За допомогою кнопки ***Додаткові параметри*** встановлюються додаткові параметри перевірки цілісності розділів та параметрів реєстру.

3.2.7.2.3.3.1.1 Встановлення переліку розділів реєстру, що підлягають перевірці

Кнопка ***Додати*** дозволяє додати розділ реєстру, який буде включено до переліку розділів, що підлягають перевірці на цілісність. Після натискання цієї кнопки на екрані з’являється діалогове вікно ***Вибір розділу реєстру*** для включення нового розділу реєстру (рисунок 3.58).

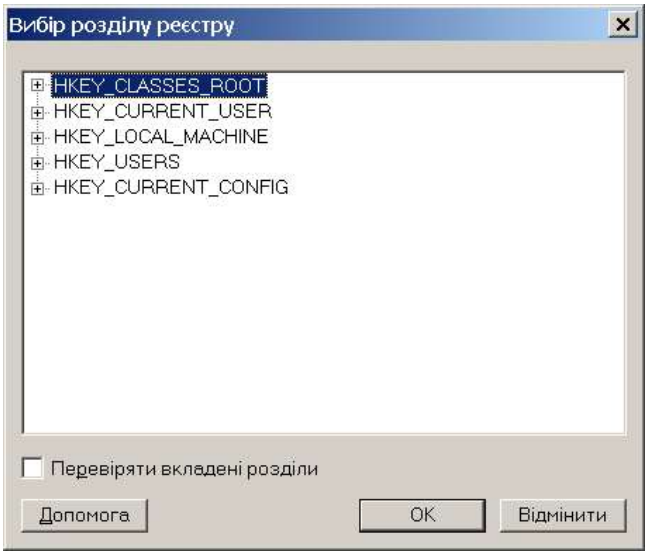

Рисунок 3.58 – Діалогове вікно для включення нового розділу до переліку розділів реєстру

Кнопка ***Видалити*** дозволяє видалити з переліку вибраний розділ реєстру після підтвердження.

Відмітка в полі ***Перевіряти вкладені розділи*** означає, що буде здійснюватись перевірка вкладених підрозділів поміченого розділу. При відсутності відмітки перевірятимуться лише такі об'єкти:

– сам розділ – на видалення та зміни дескриптора безпеки;

– параметри, що в ньому знаходяться – на зміни, видалення та створення;

– вкладені розділи першого рівня – на видалення, створення та зміни дескрипторів безпеки.

3.2.7.2.3.3.1.2 Встановлення інших параметрів

У групі ***Файл звіту про перевірку цілісності розділів та параметрів реєстру*** вводиться ім'я файлу, у який будуть записуватись результати перевірки цілісності розділів та параметрів реєстру та його граничний розмір (в КБ).

Ім'я можна ввести ручним способом або вибрати зі списку, що випадає.

У групі ***Розмір файлу*** можна встановити обмеження на розмір файлу звіту.

3.2.7.2.3.3.2 Додаткові параметри

До додаткових параметрів перевірки цілісності розділів та параметрів реєстру відносяться такі параметри:

– перелік розділів реєстру, для яких не здійснюється перевірка цілісності;

– перелік параметрів реєстру для перевірки цілісності;

– перелік параметрів реєстру, для яких не здійснюється перевірка цілісності.

Для встановлення додаткових параметрів перевірки цілісності розділів та параметрів реєстру призначене діалогове вікно ***Додаткові параметри,*** яке з'являється при натисканні кнопки ***Додаткові параметри*** на сторінці ***Реєстр*** діалогового вікна ***Параметри перевірки цілісності*** (рисунок 3.59).

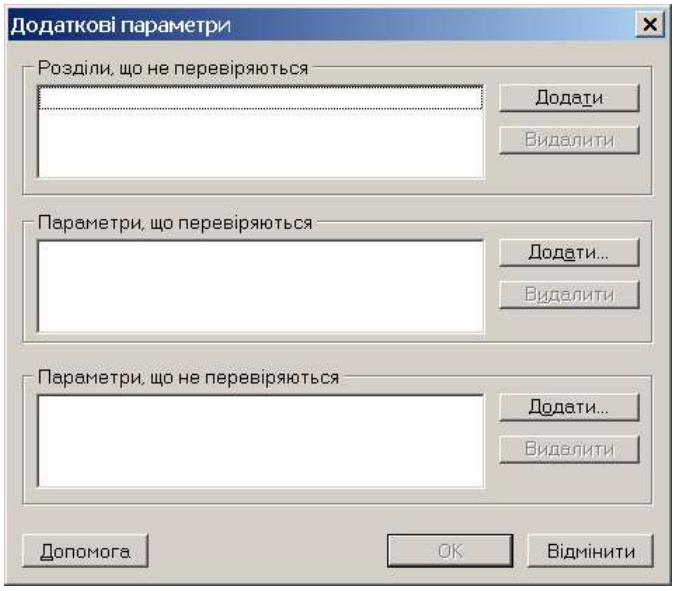

Рисунок 3.59 – Діалогове вікно для встановлення додаткових параметрів перевірки цілісності розділів та параметрів реєстру

3.2.7.2.3.3.2.1 Встановлення переліку розділів реєстру, що не підлягають перевірці

Встановлення переліку розділів реєстру відбувається за правилами, наведеними в п. 3.2.7.2.3.3.1.1.

3.2.7.2.3.3.2.2 Встановлення переліку параметрів реєстру, що підлягають та не підлягають перевірці

Кнопки ***Додати*** дозволяють додати параметр реєстру до відповідного переліку. Після натискання цих кнопок з'являється діалогове вікно ***Вибір параметра реєстру*** (рисунок 3.60).

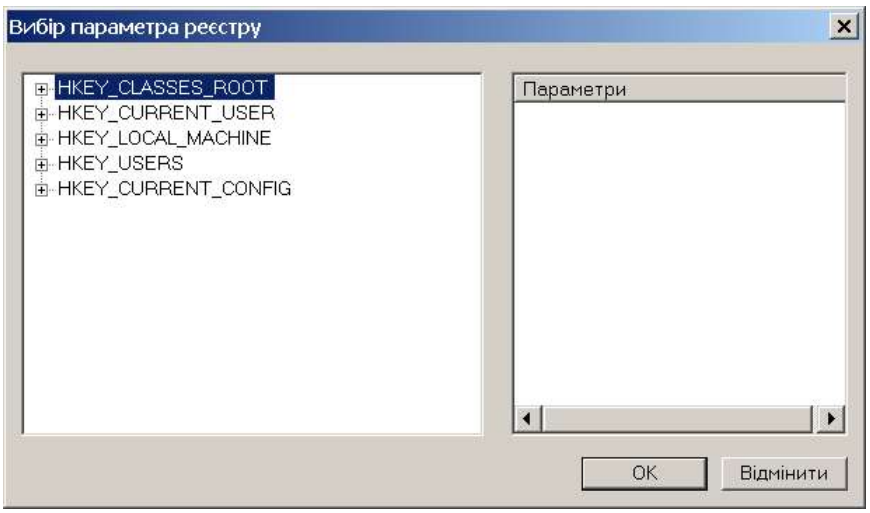

Рисунок 3.60 – Діалогове вікно для введення нового параметра реєстру

Кнопки ***Видалити*** дозволяють видалити вибраний параметр із відповідного переліку після підтвердження.

3.2.7.2.3.4 Перевірка цілісності завантажувальних секторів

До параметрів перевірки цілісності завантажувальних секторів відносяться такі параметри:

– ім'я файлу звіту про перевірку цілісності завантажувальних секторів;

– граничний розмір файлу звіту про перевірку цілісності завантажувальних секторів.

Для встановлення параметрів перевірки цілісності завантажувальних секторів призначено сторінку ***Сектори*** діалогового вікна ***Параметри перевірки цілісності*** (рисунок 3.61).

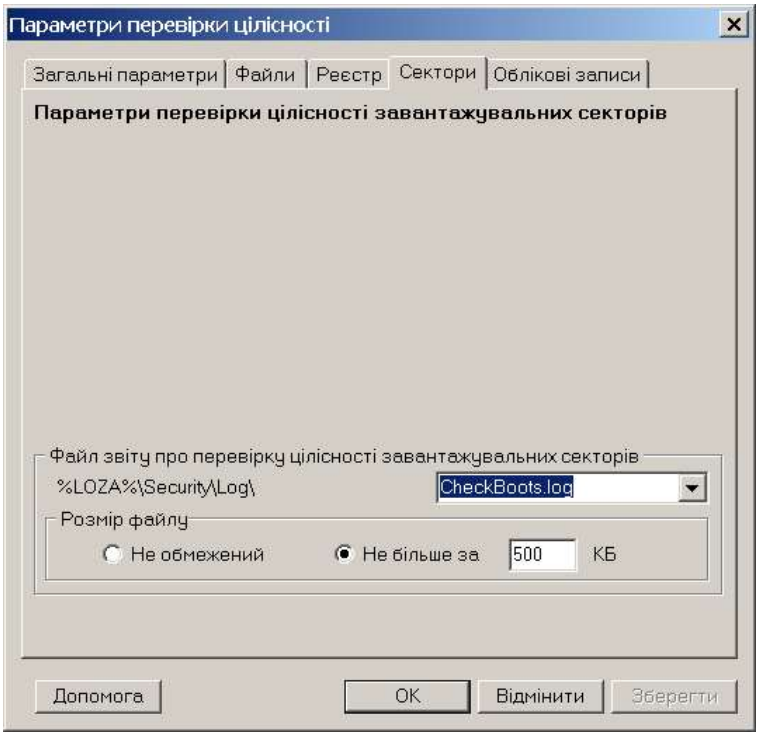

Рисунок 3.61 – Діалогове вікно для встановлення параметрів перевірки цілісності завантажувальних секторів

У групі ***Файл звіту про перевірку цілісності завантажувальних секторів*** вводиться ім'я файлу, у який будуть записуватись результати перевірки цілісності завантажувальних секторів, та його граничний розмір (в КБ).

Ім'я можна ввести ручним способом або вибрати в списку, що випадає.

У групі ***Розмір файлу*** можна встановити обмеження на розмір файлу звіту.

3.2.7.2.3.5 Перевірка цілісності облікових записів

До параметрів перевірки цілісності облікових записів відносяться такі параметри:

– перелік облікових записів, для яких не здійснюється перевірка цілісності;

– ім'я файлу звіту про перевірку цілісності облікових записів;

– граничний розмір файлу звіту про перевірку цілісності облікових записів.

Перевіряються всі облікові записи, які містяться в базі облікових записів ОС, за винятком тих, які зазначені в першому параметрі.

Для встановлення параметрів перевірки цілісності облікових записів призначено сторінку ***Облікові записи*** діалогового вікна ***Параметри перевірки цілісності*** (рисунок 3.62).

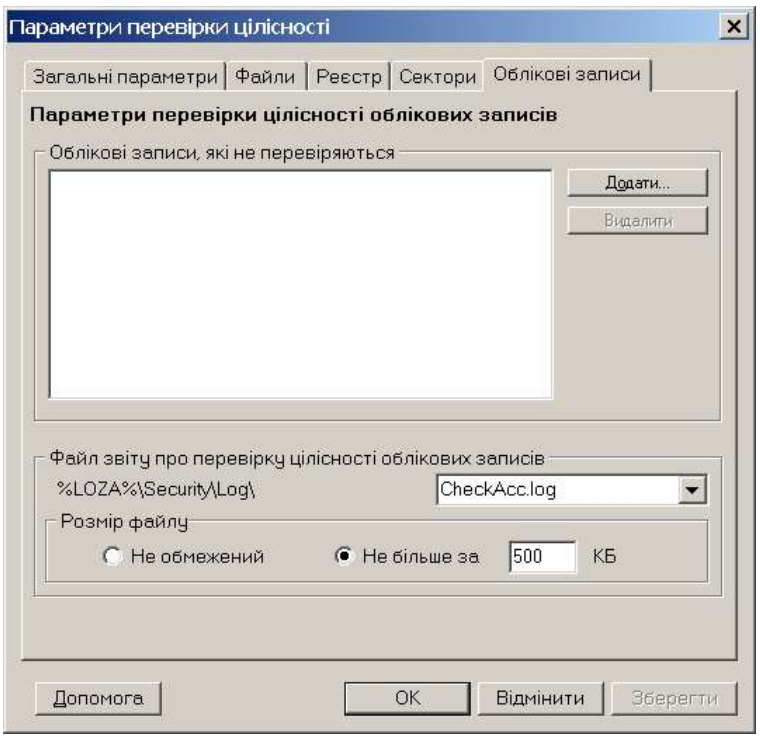

Рисунок 3.62 – Діалогове вікно для встановлення параметрів перевірки цілісності облікових записів

Кнопка ***Додати*** дозволяє додати обліковий запис, який буде включено до переліку облікових записів, які не підлягають перевірці на цілісність. Після натискання цієї кнопки на екрані з'являється діалогове вікно ***Додати обліковий запис*** для введення нового облікового запису (рисунок 3.63).

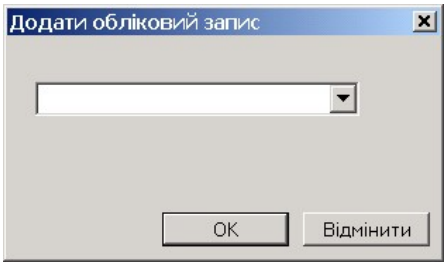

Рисунок 3.63 – Діалогове вікно для введення нового облікового запису

Кнопка ***Видалити*** дозволяє видалити з переліку вибраний обліковий запис після підтвердження.

У групі ***Файл звіту про перевірку цілісності облікових записів*** вводиться ім'я файлу, у який будуть записуватись результати перевірки цілісності облікових записів, та його граничний розмір (в КБ).

Ім'я можна ввести ручним способом або вибрати в списку, що випадає.

У групі ***Розмір файлу*** можна встановити обмеження на розмір файлу звіту.

3.2.7.2.4 Встановлення параметрів роботи з документами

3.2.7.2.4.1 Встановлення переліку дозволених шаблонів та надбудов

Під час роботи в системі користувачеві дозволяється використовувати тільки ті шаблони та надбудови, які були дозволені адміністратором безпеки. Вони встановлюються за допомогою пункту меню *Конфігурація – Параметри комп'ютера – Робота з документами – Шаблони та надбудови* або кнопки  і визначаються такими параметрами конфігурації системи:

перелік дозволених шаблонів та надбудов Word;
перелік дозволених надбудов COM для Word;
перелік дозволених шаблонів та надбудов Excel;
перелік дозволених надбудов COM для Excel.

Для встановлення цих параметрів призначене діалогове вікно Дозволені шаблони та надбудови (рисунок 3.64).

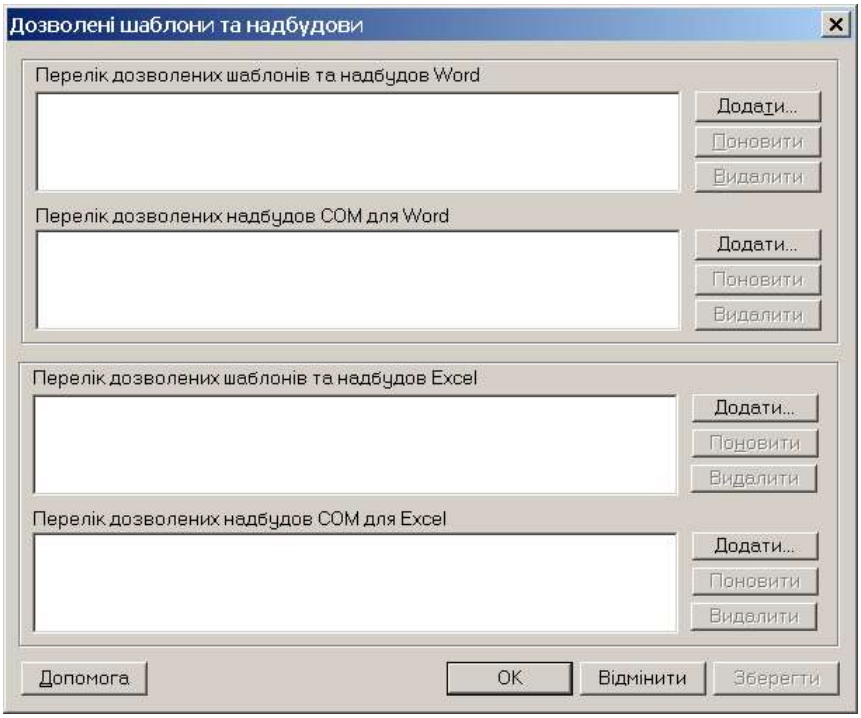

Рисунок 3.64 – Діалогове вікно для встановлення дозволених шаблонів та надбудов

Кнопки *Додати* дозволяють додати файл до відповідного переліку. При цьому підраховується та запам'ятовується його контрольна сума.

Кнопки *Поновити* дозволяють перерахувати контрольну суму вибраного файлу.

Кнопки *Видалити* дозволяють видалити вибраний файл із відповідного переліку після підтвердження.

3.2.7.2.4.2 Встановлення дисків для зберігання документів

За допомогою пункту меню *Конфігурація – Параметри комп'ютера – Робота з документами – Диски для роботи з документами* або кнопки  встановлюються такі параметри конфігурації системи:

гнучкі диски для зберігання документів;

```
знімні диски для зберігання документів;
компакт-диски для зберігання документів;
жорсткі диски для зберігання документів.
```

Для встановлення цих параметрів призначене діалогове вікно ***Диски для зберігання документів*** (рисунок 3.65).

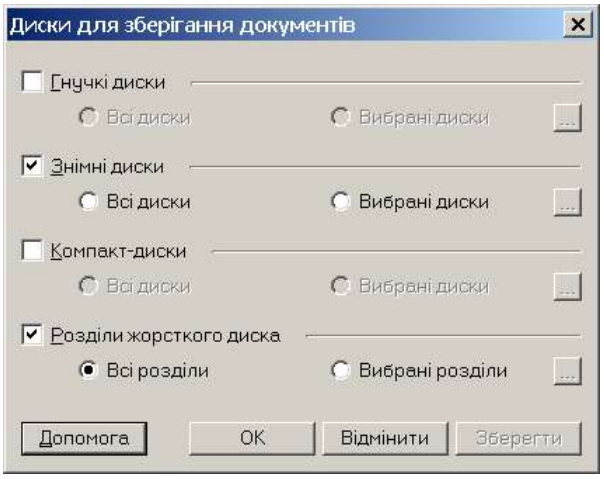

Рисунок 3.65 – Діалогове вікно для встановлення дисків для зберігання документів

Відмітки в полях ***Гнучкі диски, Знімні диски, Компакт-диски*** та ***Розділи жорсткого диска*** означають, що для зберігання документів визначаються відповідні диски. Ці параметри можуть приймати значення ***Всі диски*** або містити фіксований перелік букв, які відповідають дискам певного типу (наприклад, ***F:, G:***).

3.2.7.2.4.3 Встановлення небезпечних команд Excel

За допомогою пункту меню ***Конфігурація – Загальні параметри – Робота з документами – Небезпечні команди Excel*** або кнопки встановлюється параметр конфігурації системи `перелік небезпечних команд Excel`.

Для встановлення цього параметра призначене діалогове вікно ***Небезпечні команди Excel*** (рисунок 3.66).

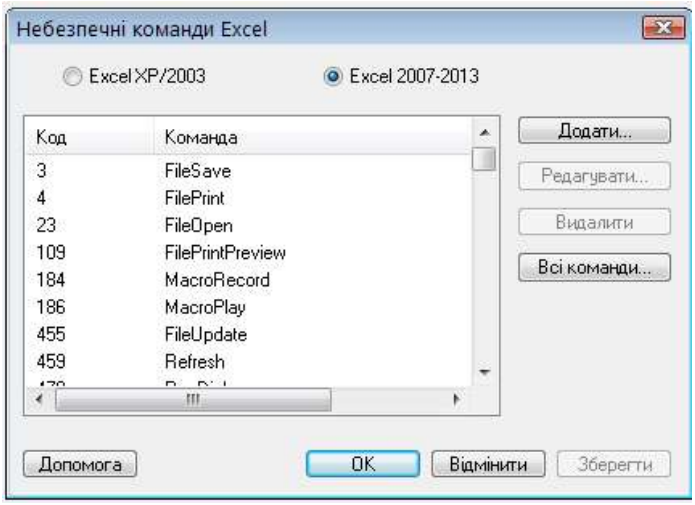

Рисунок 3.66 – Діалогове вікно для встановлення небезпечних команд Excel

За допомогою кнопки ***Додати*** можна додати команду до переліку. Після натискання цієї кнопки на екрані з'являється діалогове вікно ***Додати команду*** для введення нової команди (рисунок 3.67).

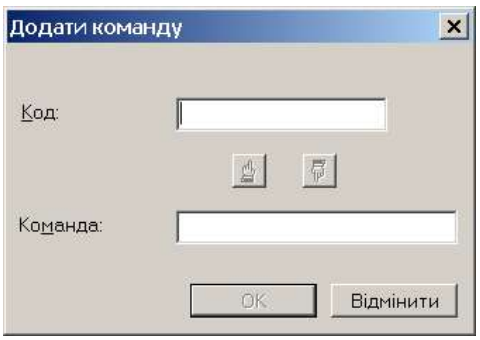

Рисунок 3.67 – Діалогове вікно для введення нової команди до переліку небезпечних команд Excel

За допомогою кнопки  можна отримати ім'я команди за вказаним кодом, за допомогою кнопки  – навпаки.

За допомогою кнопки ***Редагувати*** можна редагувати ім'я вибраної команди.

За допомогою кнопки ***Видалити*** можна видалити команду з переліку небезпечних команд. Не можна видалити команди, які встановлюються за умовчанням.

За допомогою кнопки ***Всі команди*** можна додати до переліку відразу декілька команд. Після натискання цієї кнопки на екрані з'являється діалогове вікно ***Всі команди Excel*** (рисунок 3.68).

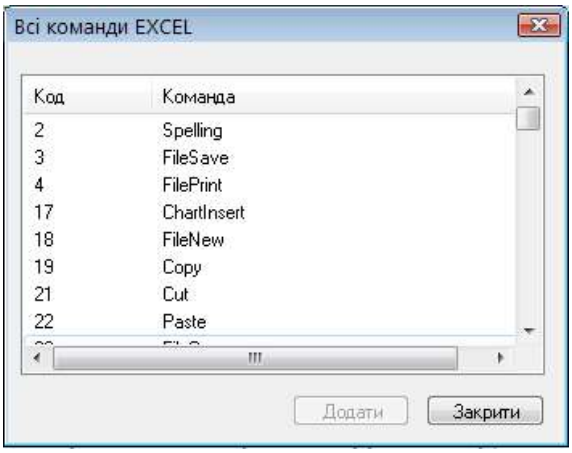

Рисунок 3.68 – Діалогове вікно для введення нових команд до переліку небезпечних команд Excel

Після натискання кнопки ***Додати*** всі відмічені команди будуть додані до переліку небезпечних команд Excel.

3.2.7.2.4.4 Встановлення небезпечних команд Word

За допомогою пункту меню ***Конфігурація – Загальні параметри – Робота з документами – Небезпечні команди Word*** або кнопки  встановлюється параметр конфігурації системи `перелік небезпечних команд Word`.

Для встановлення цього параметра призначене діалогове вікно ***Небезпечні команди Word*** (рисунок 3.69).

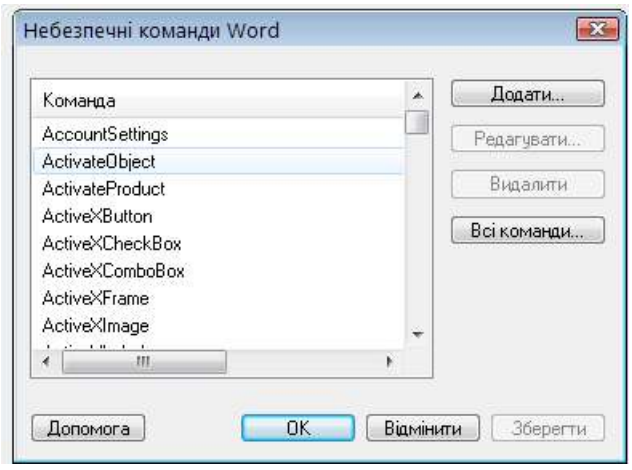

Рисунок 3.69 – Діалогове вікно для встановлення небезпечних команд Word

За допомогою кнопки ***Додати*** можна додати команду до переліку. Після натискання цієї кнопки на екрані з'являється діалогове вікно ***Додати команду*** для введення нової команди (рисунок 3.70).

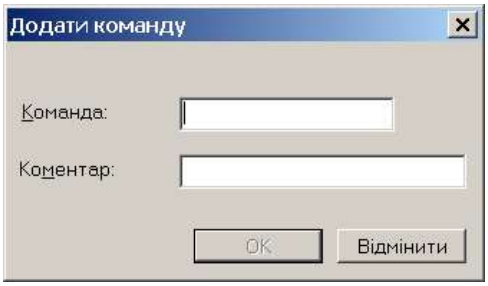

Рисунок 3.70 – Діалогове вікно для введення нової команди до переліку небезпечних команд Word

За допомогою кнопки ***Редагувати*** можна редагувати коментар вибраної команди.

За допомогою кнопки ***Видалити*** можна видалити команду з переліку небезпечних команд. Не можна видалити команди, які встановлюються за умовчанням.

За допомогою кнопки ***Всі команди*** можна додати до переліку відразу декілька команд. Після натискання цієї кнопки на екрані з'являється діалогове вікно ***Всі команди Word*** (рисунок 3.71).

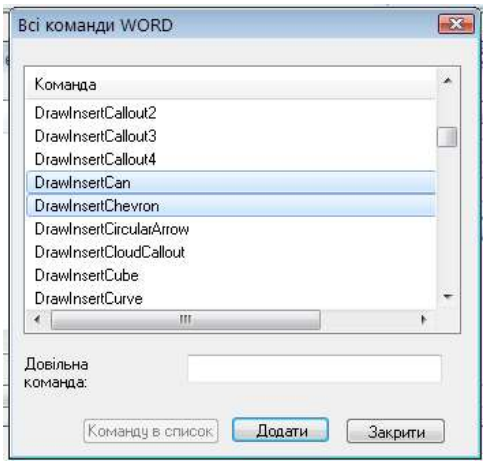

Рисунок 3.71 – Діалогове вікно для введення нових команд до переліку небезпечних команд Word

Попередньо до списку можна додати одну або кілька довільних команд (вони повинні містити латинські літери та цифри). Після натискання кнопки ***Додати*** всі відмічені у списку команди будуть додані до переліку небезпечних команд Word.

3.2.7.2.4.5 Встановлення параметрів захисту друку документів

За допомогою пункту меню ***Конфігурація – Параметри комп'ютера – Робота з документами – Захист друку документів*** або кнопки встановлюються такі параметри конфігурації системи:

– мінімальний рівень доступу для використання пароля на друк;
– захищати друк документів паролем;
– пароль на друк документів.

Для встановлення цих параметрів призначене діалогове вікно ***Захист друку документів*** (рисунок 3.72).

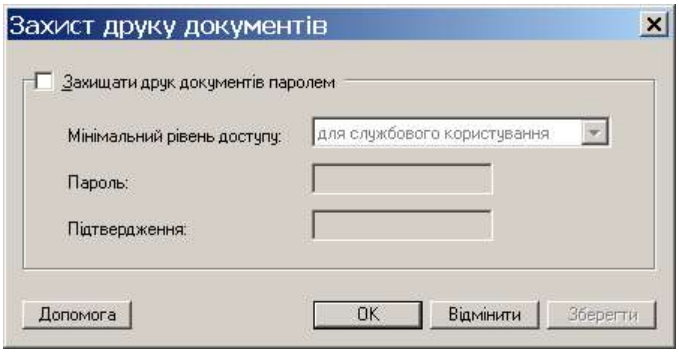

Рисунок 3.72 – Діалогове вікно для встановлення параметрів захисту друку документів

У полі ***Мінімальний рівень доступу*** вводиться мінімальний рівень доступу документів, друк яких буде захищатись паролем.

Відмітка в полі ***Захищати друк документів паролем*** забезпечує присутність представника режимно-секретного органу або іншої уповноваженої особи під час друку документів, які містять інформацію з обмеженим доступом.

У поля ***Пароль*** та ***Підтвердження*** заноситься пароль, який буде вводитись представником режимно-секретного органу або уповноваженою особою під час друку таких документів.

3.2.7.2.4.6 Встановлення параметрів захисту експорту документів

За допомогою пункту меню ***Конфігурація – Параметри комп'ютера – Робота з документами – Захист експорту документів*** або кнопки встановлюються такі параметри конфігурації системи:

– мінімальний рівень доступу для використання пароля на експорт;
– захищати експорт документів паролем;
– пароль на експорт документів.

Для встановлення цих параметрів призначене діалогове вікно ***Захист експорту документів*** (рисунок 3.73).

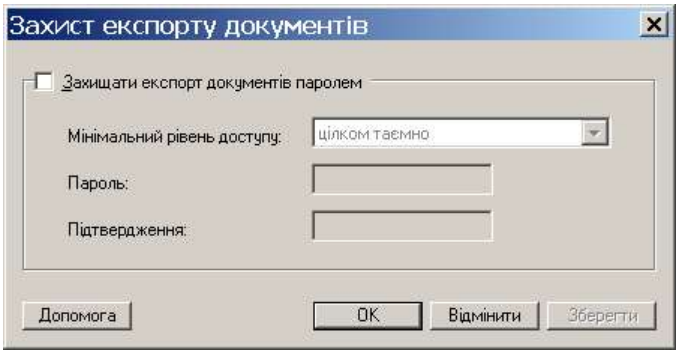

Рисунок 3.73 – Діалогове вікно для встановлення параметрів захисту експорту документів

У полі *Мінімальний рівень доступу* вводиться мінімальний рівень доступу документів, експорт яких буде захищатись паролем.

Відмітка в полі *Захищати експорт документів паролем* забезпечує присутність представника режимно-секретного органу або іншої уповноваженої особи під час експорту документів, які містять інформацію з обмеженим доступом.

У поля *Пароль* та *Підтвердження* заноситься пароль, який буде вводитись представником режимно-секретного органу або уповноваженою особою під час експорту таких документів.

3.2.7.2.5 Політика знімних дисків

За допомогою пункту меню *Конфігурація – Параметри комп'ютера – Політика знімних дисків* або кнопки встановлюються такі параметри конфігурації системи:

- політика для CD/DVD дисків;
- політика для гнучких дисків;
- політика для дисків USB Flash.

Для встановлення цих параметрів призначене діалогове вікно *Політика знімних дисків* (рисунок 3.74).

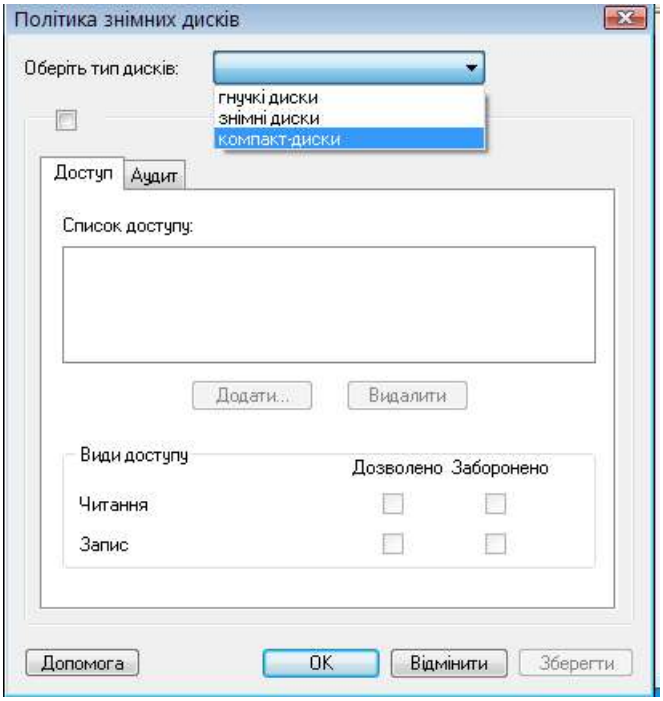

Рисунок 3.74 – Діалогове вікно для встановлення політики знімних дисків

Політика дисків може бути встановлена для кожного з таких типів знімних дисків:

– гнучкі диски (дискети);
– диски USB Flash;
– CD/DVD-диски.

Для кожного типу дисків встановлюється список доступу та список аудиту. Введення списку доступу та списку аудиту проводиться таким же чином, що і для зареєстрованих дисків USB Flash (п. 3.2.6.1).

3.2.7.2.6 Встановлення параметрів заборони друку

Система ЛОЗА-1 надає можливість повністю контролювати друк документів, які обробляються за допомогою програми *Захищені документи*. Під час обробки даних за допомогою інших програмних засобів у системі передбачена можливість повної або часткової заборони друку, а також можливість тимчасового дозволу друку.

За допомогою пункту меню *Конфігурація – Параметри комп'ютера – Заборона друку* або кнопки  встановлюються такі параметри конфігурації системи:

– спосіб заборони друку;
– облікові записи для заборони друку.

Для встановлення цих параметрів призначене діалогове вікно *Заборона друку* (рисунок 3.75).

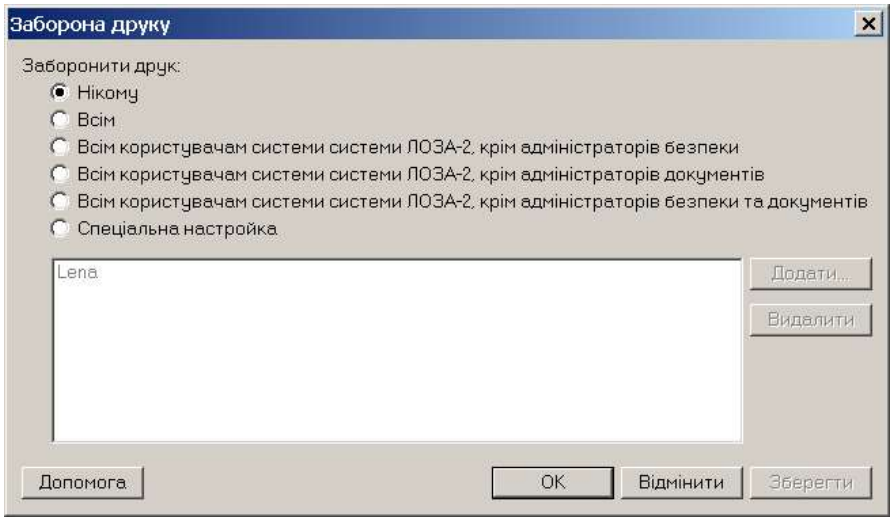

Рисунок 3.75 – Діалогове вікно для встановлення параметрів заборони друку

У разі обрання опції *Спеціальні налаштування* друк забороняється для встановленого переліку облікових записів.

За допомогою кнопки *Додати* можна додати обліковий запис до переліку облікових записів, за допомогою кнопки *Видалити* – видалити обліковий запис із переліку облікових записів.

3.2.7.2.7 Встановлення переліку заборонених програм

Перелік заборонених програм використовується для того, щоб змусити користувачів працювати з текстовими документами та електронними таблицями тільки за допомогою програми *Захищені документи*.

За допомогою пункту меню *Конфігурація – Параметри комп'ютера – Заборонені програми* або кнопки  встановлюються такі параметри конфігурації системи:

- фіксовані заборонені програми;
- додаткові заборонені програми.

За допомогою першого параметра можна заборонити виконання чотирьох стандартних програм: Microsoft Word, Microsoft Excel, Microsoft WordPad та Microsoft Блокнот.

Другий параметр дозволяє заборонити виконання будь-яких інших програм. Він містить перелік файлів, що відповідають забороненим програмам.

Для встановлення цих параметрів призначене діалогове вікно *Заборонені програми* (рисунок 3.76).

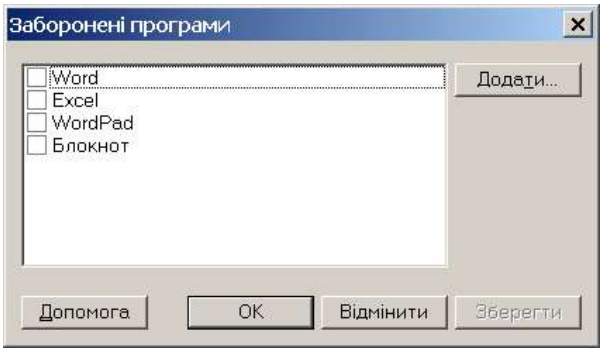

Рисунок 3.76 – Діалогове вікно для встановлення переліку заборонених програм

3.2.7.2.8 Встановлення переліку тимчасових файлів

У системі ЛОЗА-1 передбачена можливість автоматичного видалення тимчасових файлів. За допомогою пункту меню *Конфігурація – Параметри комп'ютера – Тимчасові файли* або кнопки встановлюються такі параметри конфігурації системи:

- видаляти тимчасові файли користувачів;
- перелік тимчасових файлів;
- перелік тимчасових папок.

Для встановлення цих параметрів призначене діалогове вікно *Тимчасові файли* (рисунок 3.77).

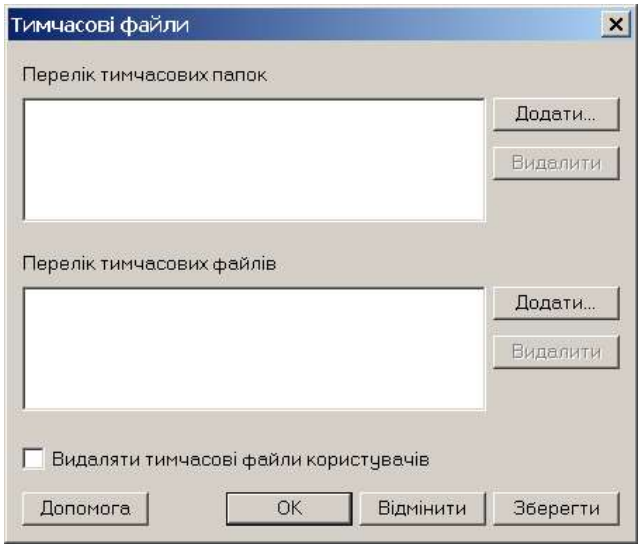

Рисунок 3.77 – Діалогове вікно для встановлення переліку тимчасових файлів

У полі *Перелік тимчасових папок* встановлюється перелік папок, які вважатимуться тимчасовими.

У полі *Перелік тимчасових файлів* встановлюється перелік файлів, які вважатимуться тимчасовими.

Відмітка в полі *Видаляти тимчасові файли користувачів* означає, що буде виконуватись автоматичне видалення тимчасових файлів та тимчасових папок разом із файлами, що в них містяться.

3.2.7.2.9 Встановлення переліку системних облікових записів

У системі ЛОЗА-1 передбачена можливість формування переліку системних облікових записів, які можна буде додавати до списку доступу та до списку аудиту. За допомогою пункту меню *Конфігурація – Параметри комп'ютера – Системні облікові записи* або кнопки  встановлюється параметр конфігурації системи `системні облікові записи`.

Для встановлення цього параметра призначене діалогове вікно *Системні облікові записи* (рисунок 3.78).

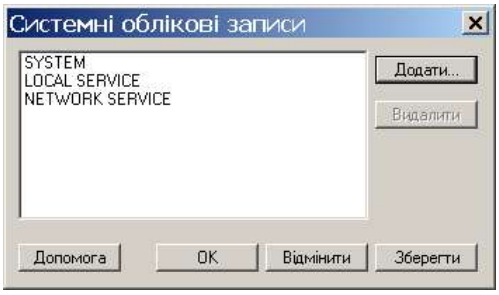

Рисунок 3.78 – Діалогове вікно для встановлення переліку системних облікових записів

За допомогою кнопки *Додати* можна додати обліковий запис до переліку системних облікових записів, за допомогою кнопки *Вилучити* – вилучити обліковий запис з переліку.

3.2.7.2.10 Визначення довірених процесів

Довірені процеси – це процеси, які не контролюються файловим драйвером системи ЛОЗА-1 для запобігання конфліктів з антивірусними програмами. Вони матимуть доступ до захищених папок користувачів і до папок самої ЛОЗИ. Для кожного процесу вказується відповідний йому файл.

Для визначення таких процесів призначене діалогове вікно *Довірені процеси* (рисунок 3.79).

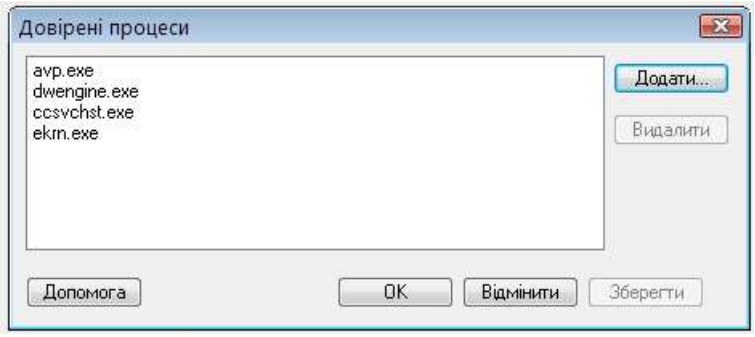

Рисунок 3.79 – Діалогове вікно для визначення списку довірених процесів системи ЛОЗА-1

3.2.7.2.11 Обробка подій

В системі передбачена можливість обробки певних подій. Загальне правило полягає в тому, що для кожної події вказується файл бібліотеки dll, яка реалізує відповідну функцію. Ця функція повинна мати фіксоване ім'я та визначення (перелік параметрів та їхніх типів, а також тип значення, яке повертає функція).

У тому випадку, коли функція повертає значення типу PWideChar, бібліотека також повинна експортувати функцію із таким визначенням:

procedure LOZAEventFreeMemory(P: Pointer); stdcall;

Далі описані технічні деталі для події створення або зміна ролі користувача.

Функція для обробки цієї події викликається у двох випадках:

– створення нового користувача (викликається після вибору імені користувача);

– зміна ролі користувача (викликається після зміни ролі користувача).

Ім’я файлу бібліотеки dll зберігається у параметрі конфігурації *Обробка події створення, перейменування або зміни ролі користувача*.

Функція, яка викликається, має таке визначення:

function LOZAEventOnCreateUser(UserName: PWideChar; UserRoles: Integer; out Options: Integer; out FullName, Description, MsgText: PWideChar; var Parameter: PWideChar; ParameterLen: Integer): Integer; stdcall;

Це визначення наведене на мові Delphi Object Pascal, але для реалізації функції може бути використана будь-яка мова програмування, яка дозволяє створення динамічних бібліотек dll для Windows.

Значення, які може повертати функція, описані далі у таблиці 3.8.

Таблиця 3.8

Значення	Пояснення
0	Створення/перейменування/зміна ролі користувача дозволяється, параметри FullName, Description можуть містити відповідно повне ім’я та опис користувача. В залежності від значення параметра Options, ці значення автоматично присвоюються відповідним властивостям користувача системи. Згодом адміністратор може змінити ці властивості користувача. Якщо параметр Options вимагає автоматичного присвоєння значень властивостям користувача, відповідне повідомлення виводиться на екран. Параметр MsgText може містити додаткове повідомлення, яке також виводиться на екран.
1	Створення/перейменування/зміна ролі користувача не рекомендується. Параметр MsgText містить відповідне повідомлення, яке виводиться на екран. Адміністратор може на власний розсуд вирішити, чи продовжувати створення/перейменування/зміну ролі користувача. Параметри FullName, Description можуть містити відповідно, повне ім’я та опис користувача. В тому випадку, коли адміністратор вирішує продовжити дію, а також в залежності від значень параметра Options (див. нижче), ці значення автоматично присвоюються відповідним властивостям користувача системи. Згодом адміністратор може змінити ці властивості користувача. Якщо параметр Options вимагає автоматичного присвоєння значень властивостям користувача, відповідне повідомлення виводиться на екран
2	Створення/перейменування/зміна ролі користувача не дозволяється, параметр MsgText містить відповідне повідомлення, яке виводиться на екран.

Параметр *Options* може містити суму декількох значень, які перелічені в таблиці 3.9.

Таблиця 3.9

Значення	Пояснення
1	Значення параметра *FullName* має бути присвоєне властивості *ім'я користувача*
2	Значення параметра *Description* має бути присвоєне властивості *опис користувача*

Для визначення цього параметра призначене діалогове вікно *Обробка подій* (рисунок 3.80).

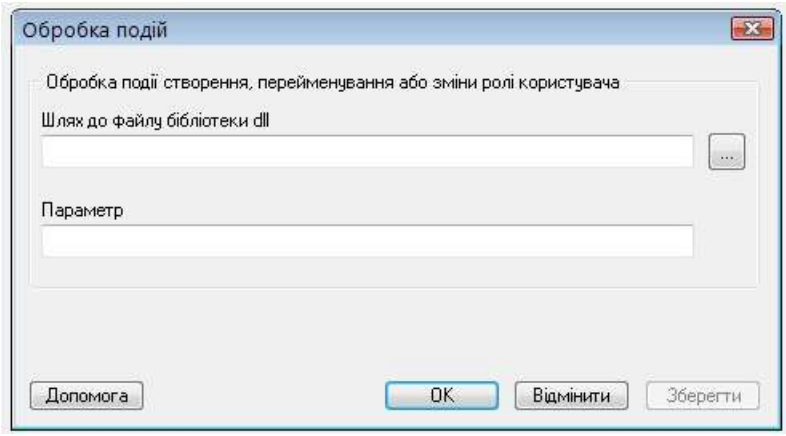

Рисунок 3.80 – Діалогове вікно для визначення параметра системи ЛОЗА-1 *Обробка подій*

3.2.7.2.12 Налаштування Windows – доступ до WPD- пристроїв

В системі, яка обробляє інформацію з обмеженим доступом, повинні бути передбачені певні обмеження при взаємодії з переносними (WPD) пристроями, такими як мобільні телефони, електронні книги, планшети тощо. Ці обмеження можуть бути реалізовані за допомогою стандартних засобів Windows – групових політик, за допомогою яких можна заборонити запис на WPD-пристрої або читання з них. Такі засоби доступні для Windows 7 та вищих версій.

ЛОЗА надає зручний інтерфейс для такої настройки за допомогою пункту меню *Конфігурація – Параметри комп'ютера – Налаштування Windows – Доступ до WPD- пристроїв* або кнопки  панелі інструментів.

Форма, за допомогою якої відбувається налаштування, наведена далі (рисунок 3.79).

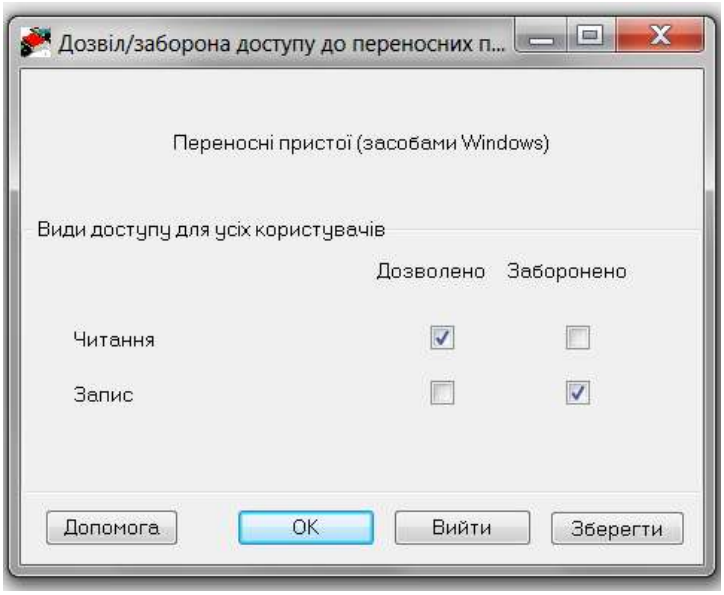

Рисунок 3.81 – Діалогове вікно для налаштування доступу до WPD - пристроїв

При такому налаштуванні, як наведено на рисунку, буде дозволено читання з WPD-пристрою та заборонений запис.

Не рекомендується одночасно використовувати настройки методами групових політик та системи ЛОЗА.

3.2.8 Встановлення значень параметрів конфігурації за умовчанням

У системі ЛОЗА-1 передбачена можливість встановлення значень параметрів конфігурації системи за умовчанням. За допомогою пункту меню *Конфігурація – Встановлення значень за умовчанням* можна встановити значення за умовчанням для одного, декількох або відразу всіх параметрів конфігурації системи.

Для встановлення значень за умовчанням призначене діалогове вікно *Встановлення значень за умовчанням* (рисунок 3.82).

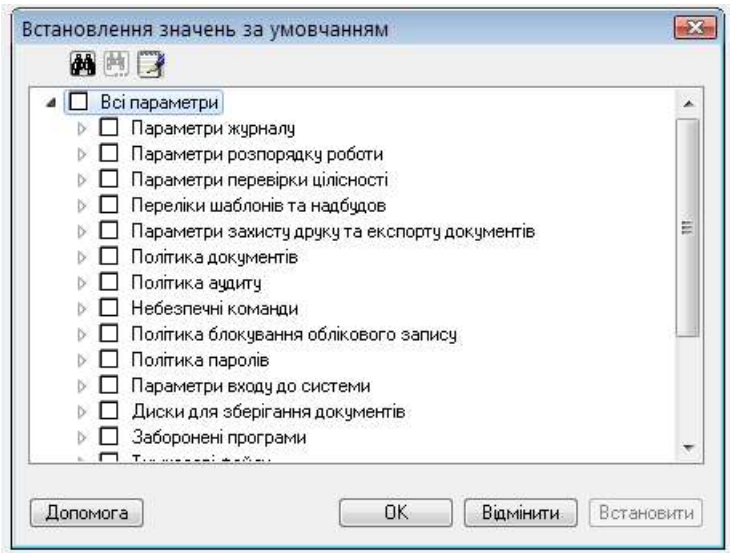

Рисунок 3.82 – Діалогове вікно для встановлення значень за умовчанням для параметрів конфігурації системи

Параметри в списку можна шукати за допомогою кнопки – почати пошук (F7). Користувач повинен вказати контекст (рисунок 3.83). Пошук буде вестись від початку списку.

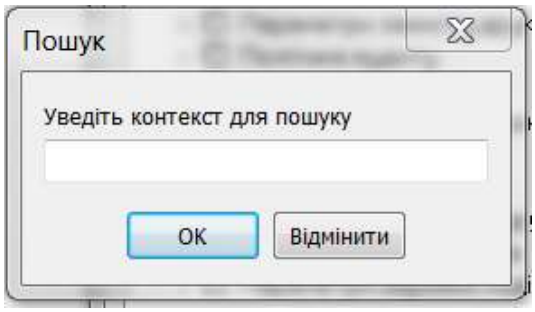

Рисунок 3.83 – Діалогове вікно для початку контекстного пошуку в списку параметрів конфігурації системи

За допомогою кнопки можна продовжити початий раніше пошук від поточного елементу списку (Ctrl + F7).

За допомогою кнопки можна викликати форму для настройки відповідного параметра. Ця можливість доступна також при подвійному натисканні кнопки миші на відповідний елемент у списку параметрів.

3.2.9 Експорт параметрів конфігурації

Після того, як на комп'ютері проведена настройка значень параметрів конфігурації, їх можна експортувати у тимчасовий файл конфігурації для подальшого використання на цьому або іншому комп'ютері, де встановлена система захисту ЛОЗА-1. Для цього потрібно скористатись пунктом меню *Конфігурація – Експорт параметрів конфігурації.* Вибір списку параметрів конфігурації, що експортуються, проводиться за допомогою форми, аналогічній наведеній на рисунку (рисунок 3.79). Далі за допомогою стандартного діалогу збереження файлу визначається файл для зберігання параметрів.

3.2.10 Імпорт параметрів конфігурації

Збережені раніше значення параметрів конфігурації можна імпортувати за допомогою пункту меню *Конфігурація – Імпорт параметрів конфігурації.* Спочатку потрібно вказати файл, де зберігаються настройки, а далі відмітити параметри, значення яких потрібно імпортувати. При цьому у формі для вибору параметрів, що імпортуються, представлені тільки ті, що містяться у тимчасовому файлі конфігурації.

3.2.11 Копіювання/відновлення службової інформації

Для полегшення процесу копіювання та відновлення службової інформації передбачено режими *Дані - Копіювання службової інформації* та *Дані - Відновлення службової інформації*.

Після входу в ці режими потрібно вибрати вид інформації для копіювання/відновлення (рисунок 3.82).

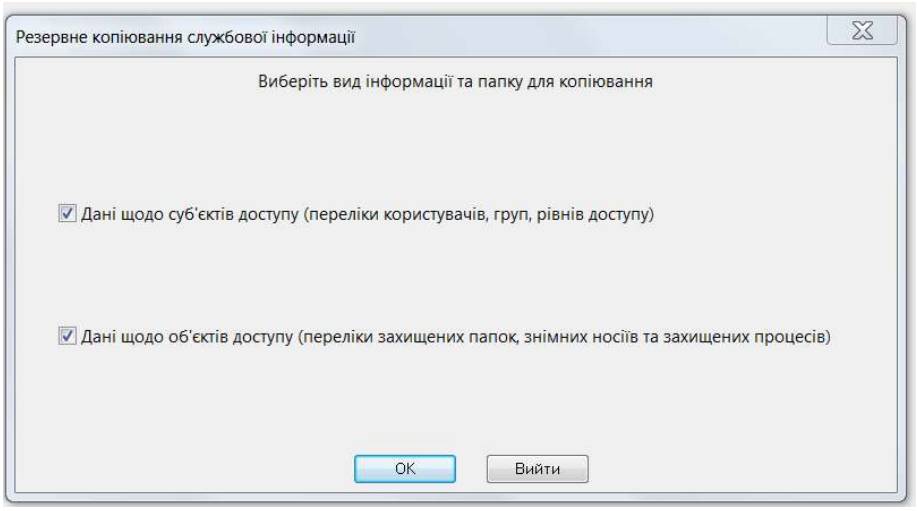

Рисунок 3.84 – Вид інформації для резервного копіювання/відновлення службової інформації

Також потрібно вибрати папку, куди копіювати/звідки брати файли. Ім’я файлу береться в залежності від виду інформації (Subjects.sqlite або Objects.sqlite).

4 Програма “Монітор захисту”

4.1 Призначення та основні функції

Програма *Монітор захисту* призначена для оперативного керування системою та спостереження за її роботою. Програма дозволяє:

– змінювати стан, у якому перебуває система;
– визначати початковий стан для наступного сеансу роботи системи;
– приймати зміни в складі програмного середовища;
– здійснювати перевірки цілісності програмного середовища;
– переглядати звіти про результати перевірок цілісності програмного середовища;
– здійснювати обробку помилок, які виникають під час виконання операцій у системі.

4.2 Робота із програмою

4.2.1 Головне вікно

Після запуску програми на екрані з’являється головне вікно (рисунок 4.1).

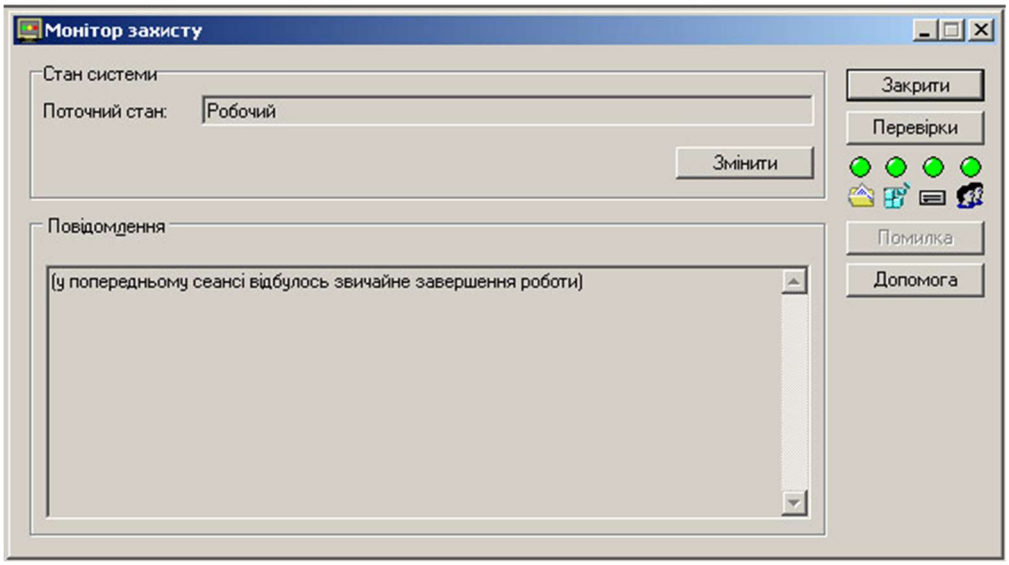

Рисунок 4.1 – Головне вікно програми

У групі *Стан системи* відображається поточний стан автоматизованої системи. Кнопка *Змінити* дозволяє змінити поточний стан системи (див. п. 4.2.2).

Поле *Повідомлення* може містити один або декілька текстових рядків з інформацією про поточну поведінку системи. У цьому полі відображаються такі дані:
– режим роботи системи (окрім режиму *перебування у певному стані*);
– підстава для зміни статусу системи (такі повідомлення наводиться в дужках);
– операції, які виконуються в системі;
– наявність помилок під час виконання операцій.

У випадку виникнення помилки поруч із переліком повідомлень з’являється відповідна піктограма й програма подає звуковий сигнал.

Індикатори під кнопкою *Перевірки* відображають стан цілісності таких об’єктів:

файли та папки;
розділи та параметри системного реєстру;

завантажувальні сектори жорстких дисків комп’ютера;
облікові записи.

4.2.2 Зміна стану системи

У групі *Стан системи* головного вікна відображається стан, у якому знаходиться система. Кнопка *Змінити* призначена для зміни стану системи вручну. Новий стан необхідно обрати в діалоговому вікні *Зміна стану* (рисунок 4.2).

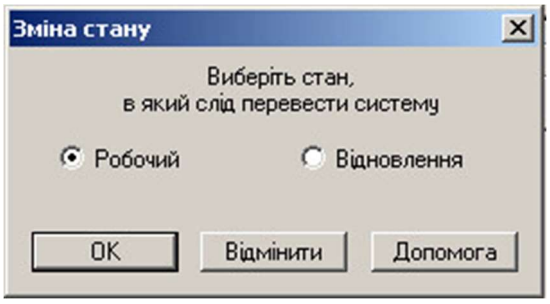

Рисунок 4.2– Діалогове вікно для вибору стану

У той час, коли система виходить із деякого стану, його назва починає блимати.

4.2.3 Перевірки цілісності

Після натискання кнопки *Перевірки* на екрані з’являється вікно *Перевірки цілісності*, за допомогою якого можна переглядати результати проведених перевірок та проводити нові перевірки.

Кожна сторінка вікна *Перевірки цілісності* відповідає одній із можливих перевірок, колір “лампочки” біля назви сторінки відображає результат перевірки. Червоне світло означає, що було виявлено порушення цілісності, зелене – що порушень не виявлено, жовте світло означає, що результат перевірки не відомий (після початку роботи системи перевірка ще не проводилась).

Необхідні відомості про перевірки цілісності наведені в документі „Загальний опис системи”.

4.2.3.1 Перевірка цілісності файлів та папок

Сторінка *Файли* вікна *Перевірки цілісності* містить інформацію про останню проведену перевірку цілісності файлів та папок (рисунок 4.3).

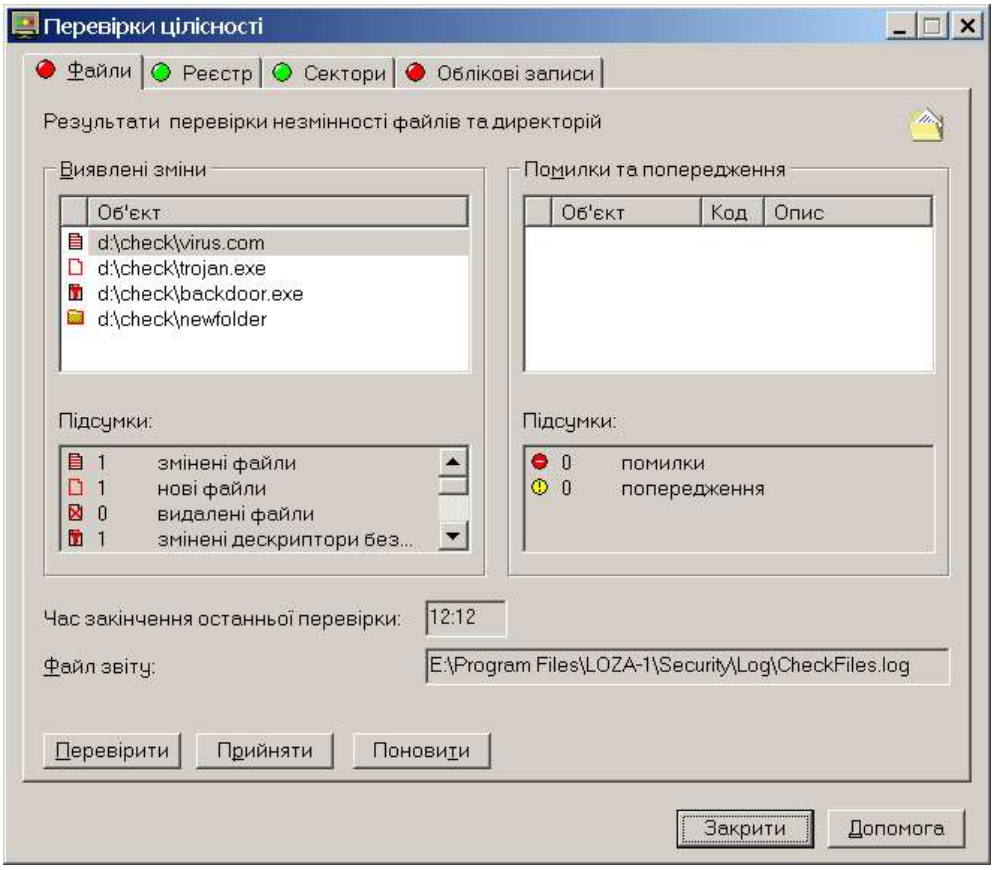

Рисунок 4.3 – Результати перевірки цілісності програмного середовища

Група ***Виявлені зміни*** містить перелік виявлених під час перевірки змін: змінені, видалені та нові файли і папки, а також файли і папки зі зміненими дескрипторами безпеки. У групі ***Підсумки*** наведена інформація про кількість об'єктів кожної групи.

Група ***Помилки та попередження*** містить інформацію про помилки та попередження, виявлені під час перевірки.

У переліках використовуються позначення, наведені в таблиці 4.1.

Таблиця 4.1 – Позначення в переліку результатів перевірки цілісності файлів та папок

Позначення	Пояснення
	змінені файли
	нові файли
	видалені файли
	змінені дескриптори безпеки файлів
	нові папки
	видалені папки
	змінені дескриптори безпеки папок
	помилки
	попередження

На цій сторінці наведено також час закінчення останньої перевірки та назву файлу, у якому було збережено звіт про перевірку.

Адміністратор може не тільки ознайомитись з результатами перевірок, проведених автоматично, а й проводити перевірки вручну та приймати зміни в складі файлів та папок.

Для ініціювання перевірки необхідно натиснути кнопку *Перевірити*. Після закінчення перевірки її результати буде відображено на сторінці.

Для прийняття змін призначено кнопки *Прийняти* та *Поновити*.

Кнопка *Прийняти* дозволяє прийняти виявлені зміни. Якщо в групі *Виявлені зміни* є відмічені рядки, приймаються лише вказані в цих рядках зміни. Якщо жодний рядок не відмічено, приймаються всі виявлені зміни.

Натискання кнопки *Поновити* призводить до повного поновлення даних про файли та папки, які підлягають перевірці на цілісність.

Проведення перевірки та прийняття змін можливе лише в тому випадку, коли система знаходиться в стані поновлення ПЗ або в стані відновлення (під час перебування системи в робочому стані та в стані профілактики перевірки проводяться автоматично).

4.2.3.2 Перевірка цілісності розділів та параметрів реєстру

Сторінка *Реєстр* вікна *Перевірки цілісності* містить інформацію про останню проведену перевірку цілісності розділів та параметрів реєстру (рисунок 4.4).

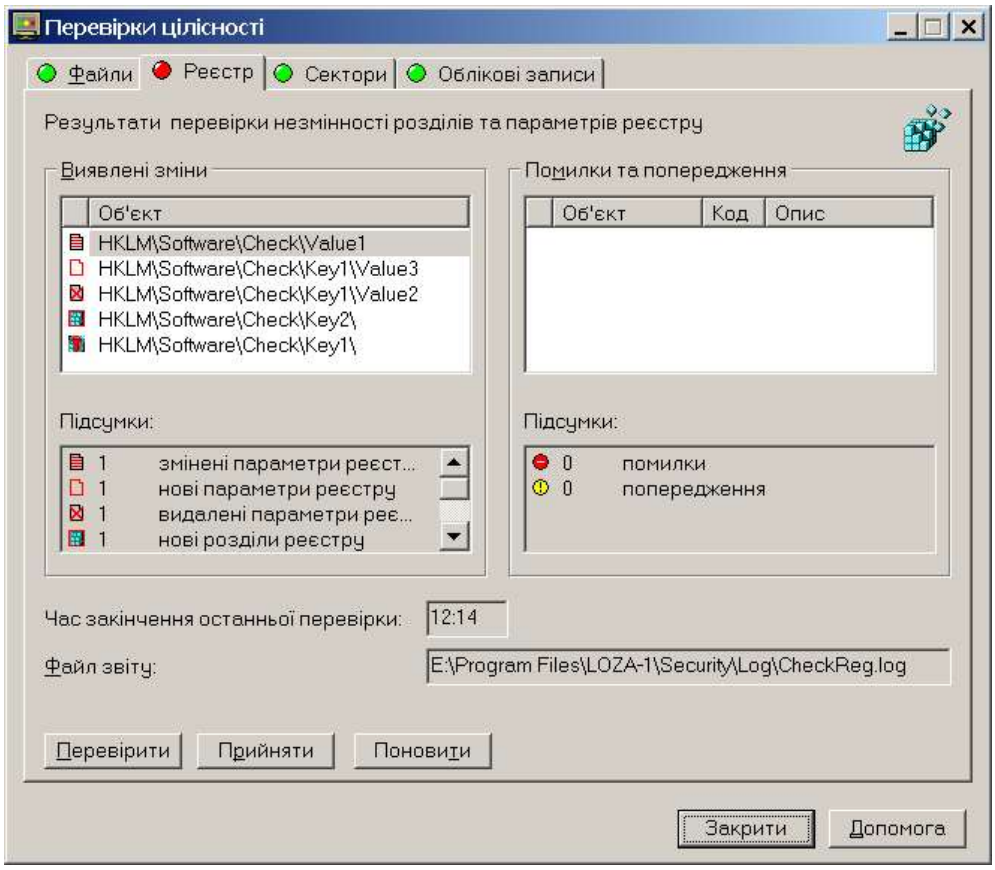

Рисунок 4.4 – Результати перевірки цілісності реєстру

Група *Виявлені зміни* містить перелік виявлених під час перевірки змін: змінені, видалені та нові параметри, нові та видалені розділи, а також розділи зі зміненими дескрипторами безпеки. У групі *Підсумки* наведена інформація про кількість об'єктів кожної групи.

Група *Помилки та попередження* містить інформацію про помилки та попередження, виявлені під час перевірки.

У переліках використовуються позначення, наведені в таблиці 4.2.

Таблиця 4.2 – Позначення в переліку результатів перевірки цілісності розділів та параметрів реєстру

Позначення	Пояснення
	змінені параметри
	нові параметри
	видалені параметри
	нові розділи
	видалені розділи
	змінені дескриптори безпеки розділів
	помилки
	попередження

На цій сторінці наведено також час закінчення останньої перевірки та назву файлу, у якому було збережено звіт про перевірку.

За допомогою кнопки *Перевірити* адміністратор може ініціювати проведення перевірки.

Кнопка *Прийняти* дозволяє адміністратору прийняти зміни. Якщо в групі *Виявлені зміни* є відмічені рядки, приймаються лише вказані в цих рядках зміни, у протилежному випадку приймаються всі виявлені зміни.

Натискання кнопки *Поновити* призводить до повного поновлення даних про розділи та параметри реєстру, які підлягають перевірці на цілісність.

Проведення перевірки та прийняття змін можливе лише в тому випадку, коли система знаходиться в стані поновлення ПЗ або в стані відновлення (під час перебування системи в робочому стані та в стані профілактики перевірки проводяться автоматично).

4.2.3.3 Перевірка цілісності завантажувальних секторів

Сторінка *Сектори* вікна *Перевірки цілісності* містить інформацію про останню проведену перевірку цілісності завантажувальних секторів (рисунок 4.5).

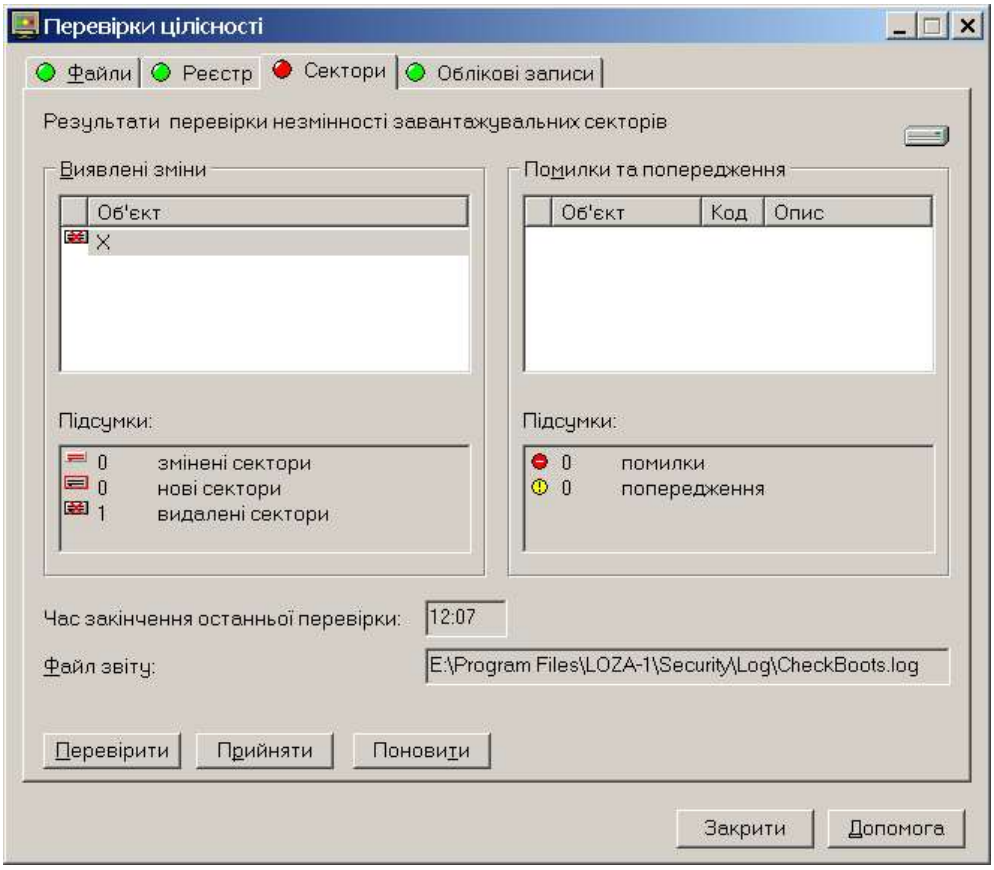

Рисунок 4.5 – Результати перевірки цілісності завантажувальних секторів

Група ***Виявлені зміни*** містить перелік виявлених під час перевірки змін: змінені, видалені та нові сектори. У групі ***Підсумки*** наведена інформація про кількість об'єктів кожної групи.

Група ***Помилки та попередження*** містить інформацію про помилки та попередження, виявлені під час перевірки.

У переліках використовуються позначення, наведені в таблиці 4.3.

Таблиця 4.3 – Позначення в переліку результатів перевірки цілісності завантажувальних секторів

Позначення	Пояснення
	змінені сектори
	нові сектори
	видалені сектори

На цій сторінці наведено також час закінчення останньої перевірки та назву файлу, у якому було збережено звіт про перевірку.

Кнопка ***Перевірити*** дозволяє провести нову перевірку, кнопка ***Прийняти*** – прийняти зміни. Якщо в групі ***Виявлені зміни*** є відмічені рядки, приймаються лише вказані в цих рядках зміни, у протилежному випадку приймаються всі виявлені зміни.

За допомогою кнопки ***Поновити*** можна повністю поновити дані про завантажувальні сектори.

Проведення перевірки та прийняття змін можливе лише в тому випадку, коли система знаходиться в стані відновлення (під час перебування системи в робочому стані перевірки проводяться автоматично).

4.2.3.4 Перевірка цілісності облікових записів

Сторінка *Облікові записи* вікна *Перевірки цілісності* містить інформацію про останню проведену перевірку облікових записів користувачів та груп (рисунок 4.6).

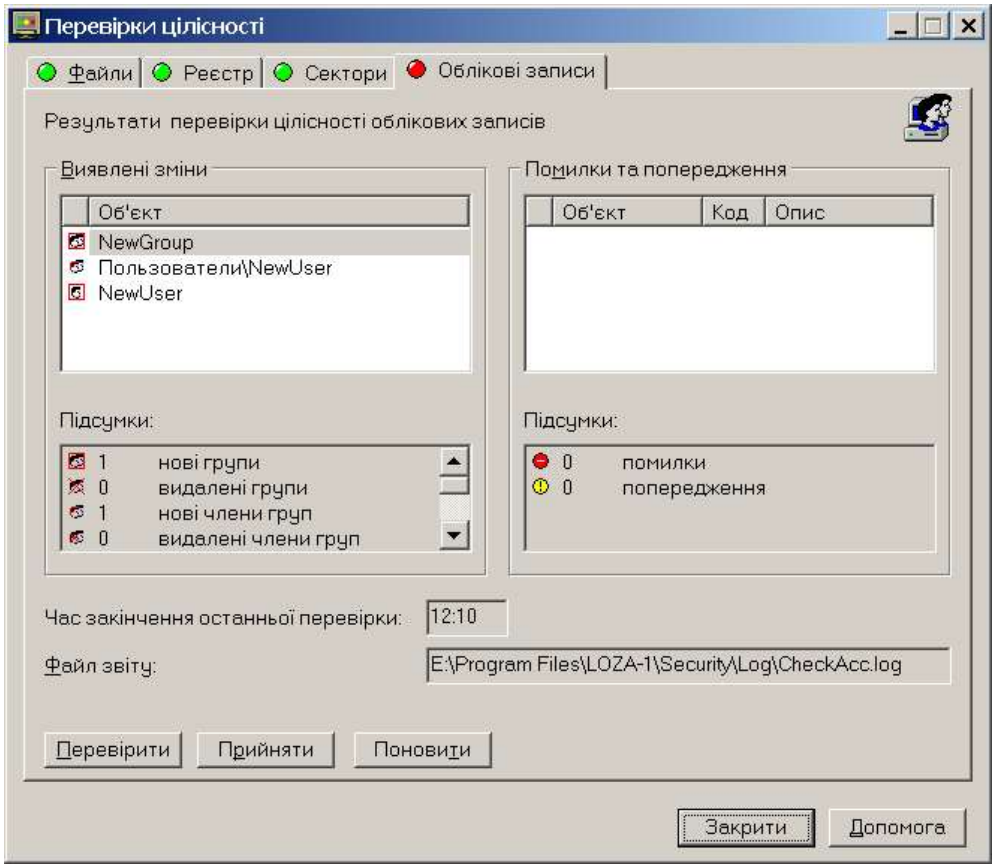

Рисунок 4.6 – Результати перевірки облікових записів

Група *Виявлені зміни* містить перелік виявлених під час перевірки змін: нові та видалені групи, нові та видалені члени груп, змінені та нові користувачі. У групі *Підсумки* наведена інформація про кількість об'єктів кожної групи.

Група *Помилки та попередження* містить інформацію про помилки та попередження, виявлені під час перевірки.

У переліках використовуються позначення, наведені в таблиці 4.4.

Таблиця 4.4 – Позначення в переліку результатів перевірки цілісності облікових записів

Позначення	Пояснення
	нові групи
	видалені групи
	нові члени груп
	видалені члени груп
	змінені користувачі
	нові користувачі
	помилки
	попередження

На цій сторінці наведено також час закінчення останньої перевірки та назву файлу, у якому було збережено звіт про перевірку.

За допомогою кнопки *Перевірити* адміністратор може ініціювати проведення перевірки.

Кнопка *Прийняти* дозволяє адміністратору прийняти зміни. Якщо в групі *Виявлені зміни* є відмічені рядки, приймаються лише вказані в цих рядках зміни, у протилежному випадку приймаються всі виявлені зміни.

Натискання кнопки *Поновити* призводить до повного поновлення даних про розділи та параметри реєстру, які підлягають перевірці на цілісність.

Проведення перевірки та прийняття змін можливе лише в тому випадку, коли система знаходиться в стані відновлення (під час перебування системи в робочому стані перевірки проводяться автоматично).

4.2.4 Обробка помилок

Порядок обробки помилок, які виникають під час виконання операцій, докладно описано в документі “Загальний опис системи”.

У випадку виникнення помилки в головному вікні програми *Монітор захисту* з’являється повідомлення про це, як зображено далі (рисунок 4.7) і стає доступною кнопка *Помилка*.

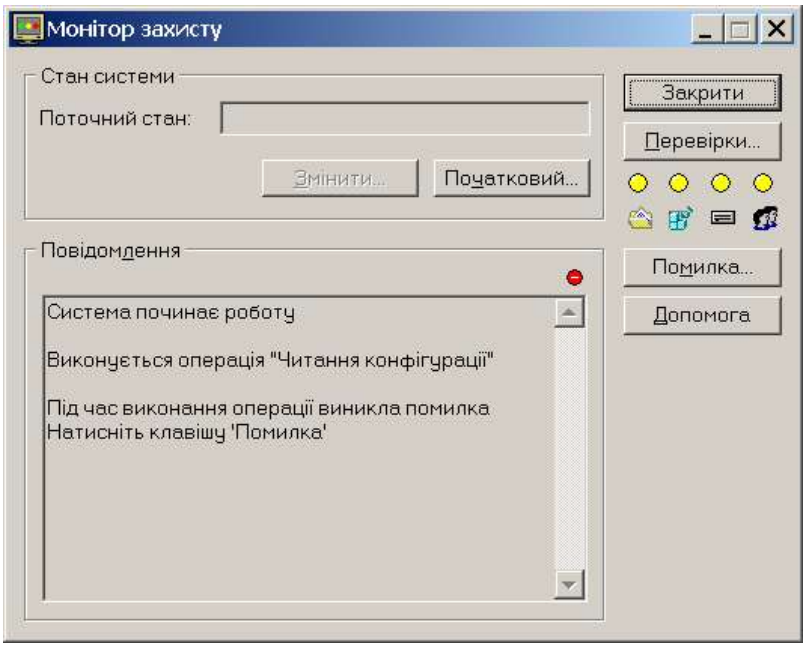

Рисунок 4.7 – Повідомлення про помилку у головному вікні

Після натискання кнопки *Помилка* з’являється вікно (рисунок 4.8), яке дозволяє обрати спосіб обробки помилки.

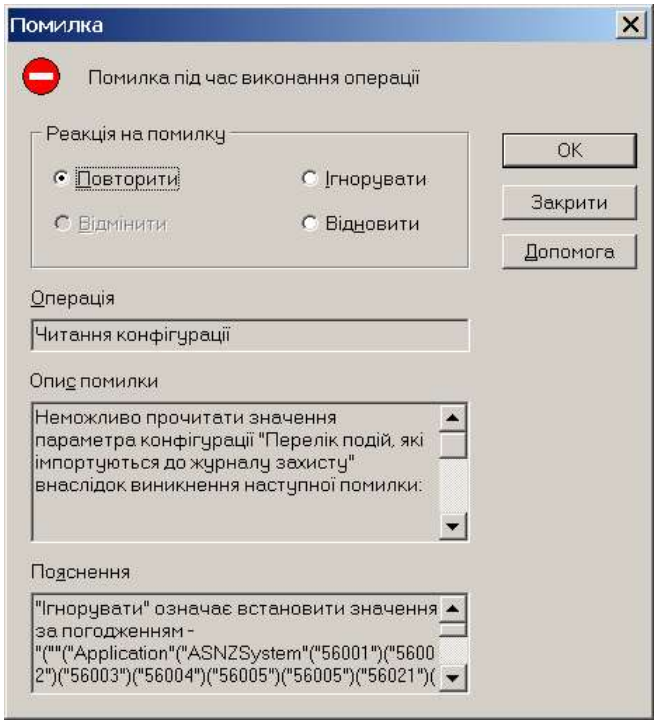

Рисунок 4.8 – Опис помилки

У переліку можливих реакцій на помилку доступними є лише ті, які можуть бути застосовані для даної помилки.

У цьому ж вікні наведено назву операції, під час виконання якої виникла помилка, та докладний опис помилки.

Для деяких операцій варіанти реакції на помилку потребують пояснення. Такі пояснення виводяться в нижній частині вікна *Помилка* (рисунок 4.8).

5 Додаткові програмні засоби

5.1 Програма «Помічник адміністратора»

Програма *Помічник адміністратора* (файл %LOZA%\LIB\AdminAssistant.exe) призначена для вирішення деяких додаткових адміністративних завдань.

Програма призначена для роботи адміністратора безпеки. Адміністратор безпеки може запустити її під час роботи іншого користувача, не примушуючи його виходити із системи. У цьому випадку після запуску програми відображається діалог входу до системи ЛОЗА-1, який пропонує адміністратору вказати своє ім'я, пароль та (за необхідності) встановити ключовий диск.

Головне вікно програми містить дві закладки: *Заборона друку* та *Бази документів*.

5.1.1 Заборона друку

Натиснувши кнопку *Дозволити друк* на закладці *Заборона друку* (рисунок 5.1), адміністратор може тимчасово дозволити друк, який був заборонений за допомогою параметра конфігурації `спосіб заборони друку` та `облікові записи для заборони друку` (див. п. 3.2.7.2.6). Перед натисканням кнопки адміністратор може обрати один із двох варіантів надання дозволу на друк:

– дозволити друк, поки сам адміністратор його не заборонить за допомогою кнопки *Заборонити друк*;

– дозволити друк, поки встановлений ключовий диск адміністратора.

Рекомендується обирати другий варіант дозволу друку. Цей варіант означає, що система автоматично відновить заборону друку, щойно адміністратор вийме свій ключовий диск.

Якщо адміністратор не відновив заборону друку, вона буде відновлена автоматично під час наступного входу будь-якого користувача до системи.

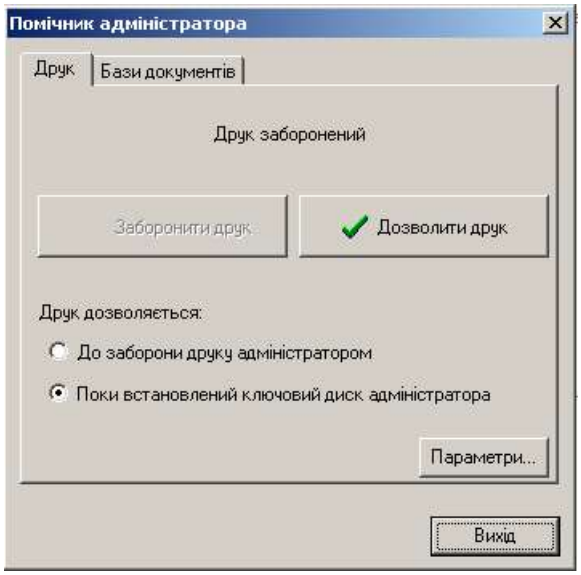

Рисунок 5.1

5.1.2 Бази документів

Під час перебування системи ЛОЗА-1 у робочому стані доступ до папок, в яких зберігаються бази документів (папки LOZADOC у кореневих папках відповідних дисків), унеможливлюється за рахунок використання засобів системи ЛОЗА-1. Для

виконання резервного копіювання баз документів та відновлення баз документів після збоїв (див. п. 4.2.2) систему необхідно перевести у стан відновлення. Бази документів, які зберігаються на знімних дисках, після цього стають доступними, а для отримання доступу до баз документів, які зберігаються на розділах жорсткого диска, треба виконати ще деякі дії. Це пов'язане із тим, що для захисту цих баз використовується додатковий засіб – встановлення дозволів NTFS.

Програма ***Помічник адміністратора*** надає можливість зручним чином змінити дозволи на доступ до відповідної папки таким чином, щоб з нею міг працювати адміністратор безпеки. Для цього досить натиснути кнопку ***Дозволити друк*** на сторінці ***Бази документів*** (рисунок 5.2). Перед натисканням кнопки адміністратор може обрати один із двох варіантів надання дозволу на друк:

– дозволити доступ, поки сам адміністратор його не заборонить за допомогою кнопки ***Заборонити доступ***;

– дозволити доступ, поки встановлений ключовий диск адміністратора.

Рекомендується обирати другий варіант дозволу доступу. Цей варіант означає, що система автоматично відновить заборону доступу, щойно адміністратора вийме свій ключовий диск.

Якщо адміністратор не відновив заборону доступ до баз документів, вона буде відновлена автоматично під час наступного входу будь-якого користувача до системи.

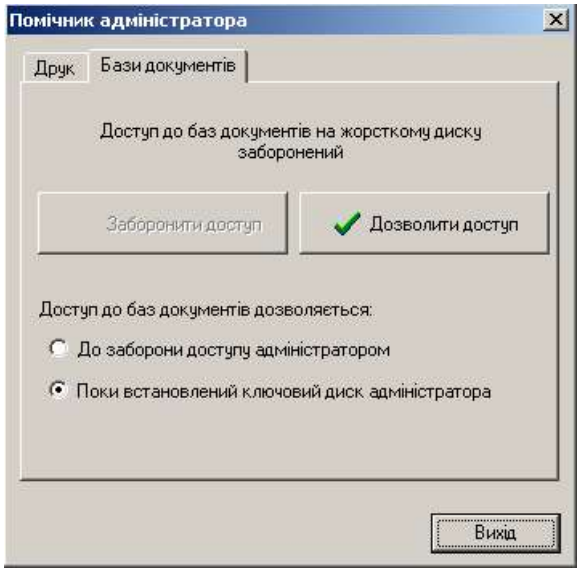

Рисунок 5.2

5.2 Програма «Перетворення формату службових файлів, отриманих у попередніх версіях системи»

Програма ***Перетворення формату службових файлів, отриманих у попередніх версіях системи*** (файл *%LOZA%\LIB\Convertorcds_sdt.exe*) призначена для підготовки імпорту службових файлів (списків користувачів, захищених папок, процесів тощо), отриманих шляхом експорту у системі ЛОЗА-1 версії 2 або 3. Вони мають розширення .cds і потребують спеціальних засобів для своєї обробки. При імпорті/експорті у системі ЛОЗА-1 версії 4 використовується спеціальний текстовий формат (розширення .sdt).

Програма є консольним додатком та використовує такі параметри:

– вхідний cds-файл або директорія, що містить файли;

– результат (якщо не вказаний, то файли записуються у ту ж саму директорію і під тим ж іменами, що і вхідні, змінюється тільки розширення файлів);

– опції (не обов’язково).

Опції можуть включати:

– notReplaceIfExists – не заміщати, якщо файл існує (за умовчанням відбувається заміщення);

– notTab – не використовувати Tab як розділювач полів (для імпорту списків цю опцію не потрібно вказувати);

– outMess – видача повідомлень про хід виконання програми (за умовчанням видача не передбачена).

Приклади використання програми (наприклад, за допомогою командного рядка Windows):

"%LOZA%\LIB\Convertorcds_sdt.exe" d:\Temp\Lists – будуть перетворені у новий формат усі cds-файли з папки d:\Temp\Lists і розміщені там же;

"%LOZA%\LIB\Convertorcds_sdt.exe" d:\Temp\Lists\UserList.cds d:\Temp\Lists\UserList1.sdt –outMess – буде перетворений у новий формат файл d:\Temp\Lists\UserList.cds, користувач отримуватиме повідомлення від програми.

Перелік скорочень

АС – автоматизована система
ОС – операційна система
ПЗ – програмне забезпечення
%LOZA% – коренева папка системи

Параметри конфігурації системи виділено `рівномірним шрифтом`.