Товариство з обмеженою відповідальністю
Науково-дослідний інститут
«Автопром»

Система захисту інформації

ЛОЗА™-1

версія 3.2.0

ПРОГРАМНІ ЗАСОБИ АДМІНІСТРУВАННЯ СИСТЕМИ

ІНСТРУКЦІЯ КОРИСТУВАЧА

ЛОЗА-1.І3.06.2

ТОВ НДІ “Автопром”
Київ, 2012

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 XP/Vista/7;

– Microsoft Word та Microsoft Excel із набору MS Office версії XP/2003/2007/2010.

2 Програма *Аудитор*

2.1 Призначення та основні функції

Програму *Аудитор* призначено для роботи з *журналом реєстрації подій*. Цей журнал формується з подій аудита, 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 з 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 структуру головного меню програми.

Таблиця. 2.1 – Структура головного меню програми *Аудитор*

Меню	Підменю	Кнопка	Дія
Журнал	Журнал реєстрації		Відкрити журнал реєстрації подій
	Відкрити		Відкрити файл журналу
	Додати файл журналу		Додати файл журналу до відкритого файлу
	Зберегти як		Зберегти журнал у файлі
	Очистити		Очистити весь журнал
	Вихід Alt+F4		Закінчити роботу з програмою
Вигляд	Всі події		Зняти умови відбору подій
	Фільтр		Встановити умови відбору подій
	Спочатку нові		Сортувати події у порядку зростання дат
	Спочатку старі		Сортувати події у порядку спадання дат
	Пошук CTRL+F		Почати пошук подій за встановленими умовами
	Пошук далі F3		Продовжити пошук за встановленими умовами
	Відомості… Enter		Переглянути опис події
	Поновити дані F5		Поновити дані в журналі
Протоколи	Звіт про небезпечні події		Сформувати звіт про небезпечні події
	Протокол друку		Сформувати протокол друку

Меню	Підменю	Кнопка	Дія
	Протокол за вибором		Сформувати протокол відстеження подій
Параметри	Зберігати настройку при виході		Зберігати настройки фільтра, пошуку, порядок сортування подій, а також розміри та місце положення головного вікна програми при виході з програми
	Шрифт		Вибирати шрифт для перегляду журналу
Допомога	Зміст F1		Переглянути файл допомоги
	Про програму		Переглянути загальну інформацію про програму

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;
- час;
- джерело;
- категорія;
- код події;
- ім’я користувача;
- ім’я комп’ютера.

На рисунку 2.1 наведено головне вікно програми.

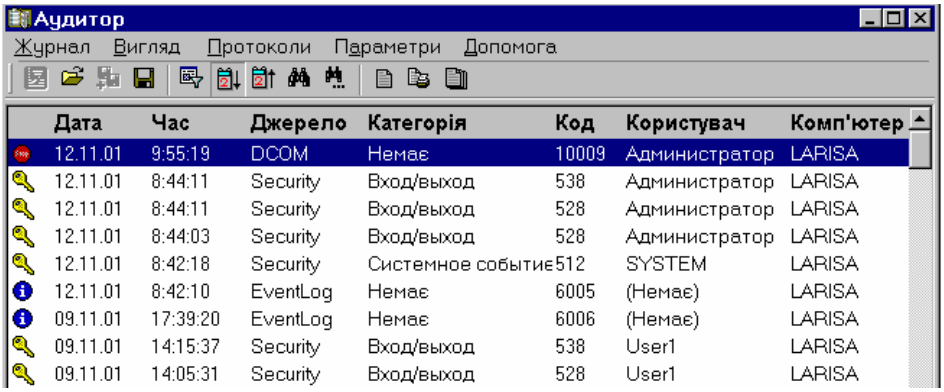

Рисунок 2.1 – Головне вікно програми *Аудитор*

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

Таблиця 2.2 – Можливі типи подій

Позначка	Тип події	Значення

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.

Для того щоб переглянути опис події, треба вибрати цю подію та виконати 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).

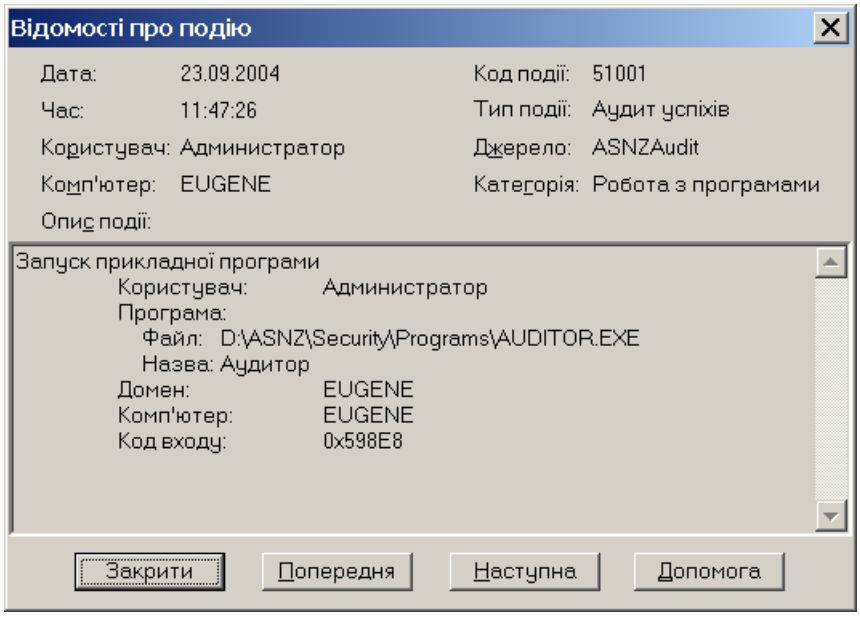

Рисунок 2.2 – Діалогове вікно для перегляду відомостей про подію

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

Порядок сортування подій встановлюється за допомогою пунктів меню *Вигляд – Спочатку старі* або кнопки (сортування у хронологічному порядку) та *Вигляд – Спочатку нові* чи кнопки (сортування у зворотному хронологічному порядку).

2.2.1.2 Фільтрування подій

Фільтрування подій полягає в тому, що на екран виводиться не весь журнал, а лише ті події, які задовольняють певним умовам.

Якщо фільтрування встановлено, пункт меню *Вигляд – Фільтр* буде помічено, а в заголовку головного вікна програми з'явиться слово "Фільтр".

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).

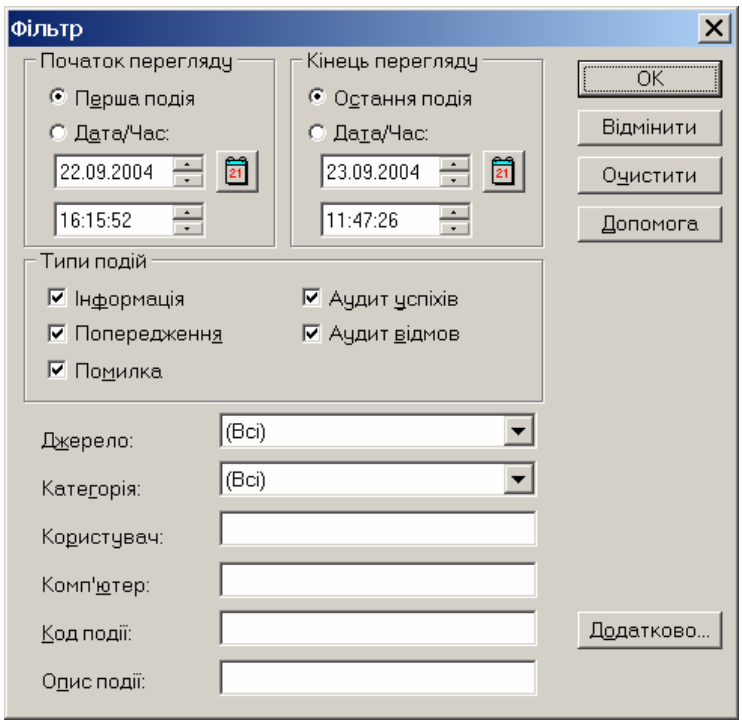

Рисунок 2.3 – Діалогове вікно для формування умов відбору подій

Групи *Початок перегляду* та *Кінець перегляду* дозволяють встановити інтервал дат для перегляду подій.

Якщо в групі *Початок перегляду* вибрано значення *Перша подія*, перегляд відбуватиметься від початку журналу, вибір значення *Дата/Час* вказує на те, що перегляд слід почати від вказаної дати та часу включно.

При натисканні кнопки на екрані з'являється вікно з календарем, за допомогою якого можна вибрати дату.

Група *Кінець перегляду* дозволяє аналогічним чином визначити кінець інтервалу дат та часу для перегляду подій.

Група *Типи подій* дозволяє вибрати декілька можливих типів подій.

Поля *Джерело, Категорія, Користувач, Комп'ютер, Код події* дозволяють зафіксувати відповідні атрибути із заголовка події.

Поле *Опис події* дозволяє вказати текст, який має міститись в описі події.

Поля *Користувач, Комп'ютер, Код події* та *Опис події* можна залишити незаповненими, а в полях *Джерело* та *Категорія* вибрати значення *(Всі)*. У цьому випадку під час відбору подій вони не використовуватимуться.

Поля *Користувач*, *Комп'ютер* та *Опис події* нечутливі до регістру.

Щоб поновити стандартні умови відбору подій (перегляд усього журналу), треба натиснути кнопку *Очистити*.

Для подій *Спроба друку екранної форми LOZAAudit* (категорія *Доступ до вихідних форм*, код 52004) та *Спроба друку документа* (категорія *Доступ до документів*, код 58004) джерела *LOZAAudit* за допомогою кнопки *Додатково* вікна *Фільтр* можна вказати більш докладні умови відбору. Після натискання кнопки *Додатково* на екрані з'являється діалогове вікно *Додаткові дані про подію* (рисунок 2.4).

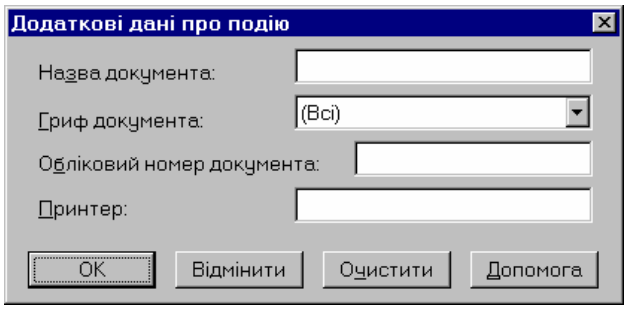

Рисунок 2.4 – Діалогове вікно для формування додаткових даних про подію *61005*

У полях цього вікна вказується назва документа, його гриф, обліковий номер та ім'я принтера. Гриф документа можна вибрати з переліку, що випадає в цьому полі (усі дані вказувати не обов'язково).

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 *Пошук* (рисунок 2.5).

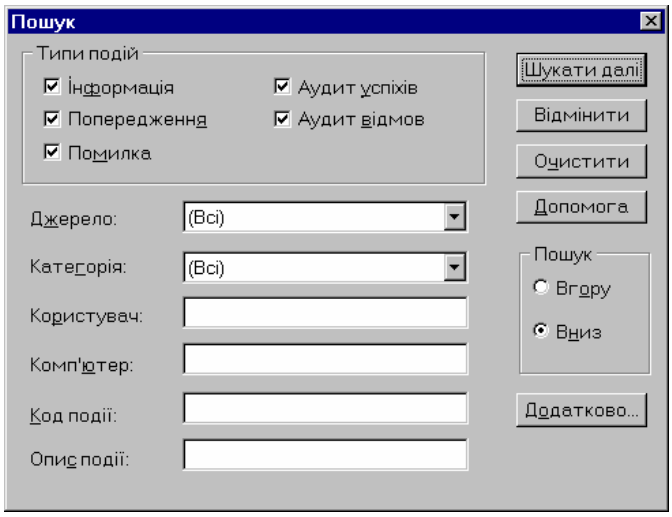

Рисунок 2.5 – Діалогове вікно для формування умов пошуку подій

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

Можна вказати також напрям пошуку, вибираючи значення *Вгору* або *Вниз*.

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 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.

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*.

При збереженні журналу зберігається весь журнал незалежно від встановленого фільтра.

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. Меню *Журнал – Додати файл журналу* та відповідна кнопка  стають доступними лише тоді, коли вже відкрито файл журналу, до поточного журналу додавати файл журналу не можна.

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 файлами журналу реєстрації.

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 за вибором (містить події, які відбираються за вказаними критеріями, наприклад, за всіма подіями, за якоюсь подією, за категорією подій, за діями певного користувача та ін.).

Форми звіту про небезпечні події та протоколу друку наведено в документі “Загальний опис системи”. Форма протоколу за вибором змінюється в залежності від указаних умов.

Сформовані протоколи та звіти зберігаються у форматі RTF, а для їхнього перегляду та друку можна використовувати, наприклад, текстовий процесор MS Word.

2.2.3.1 Звіт про небезпечні події

Звіт про небезпечні події може бути сформований за допомогою пункту меню *Протоколи – Звіт про небезпечні події* або кнопки  (цей самий звіт формується автоматично під час роботи системи у випадку виникнення відповідних подій).

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

– час початку роботи системи;

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

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

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

2.2.3.2 Протокол друку документів

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

Він може формуватись за датою або за інтервалом дат, що визначається в діалоговому вікні *Протокол друку* (рисунок 2.6).

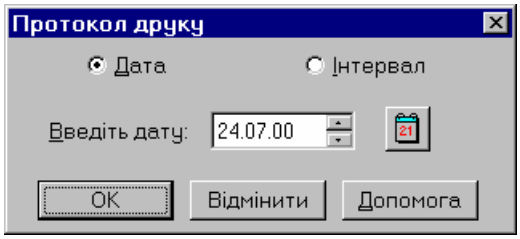

Рисунок 2.6 – Діалогове вікно для формування умов відбору до протоколу друку

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*.

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

– обрану дату або інтервал дат;

– ім’я комп’ютера, на якому надруковано документ;

– 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 (якщо задано інтервал дат) та час друку документа;

– ім’я користувача, що друкував документ;
– принтер, на якому надруковано документ;
– мітка носія даних, з якого друкувався документ;
– назву документа;
– гриф документа;
– обліковий номер документа;
– кількість аркушів в одному примірнику;
– кількість примірників.

Якщо задано інтервал дат, протокол друку містить для кожної дати з інтервалу підсумковий рядок із кількістю аркушів, надрукованих протягом дня.

2.2.3.3 Протокол за вибором

Протокол за вибором формується за допомогою пункту меню *Протоколи – Протокол за вибором* або кнопки  . Діалогове вікно *Протокол за вибором* (рисунок 2.7) аналогічне вікну *Фільтр*, воно дозволяє сформувати умови відбору подій для протоколу.

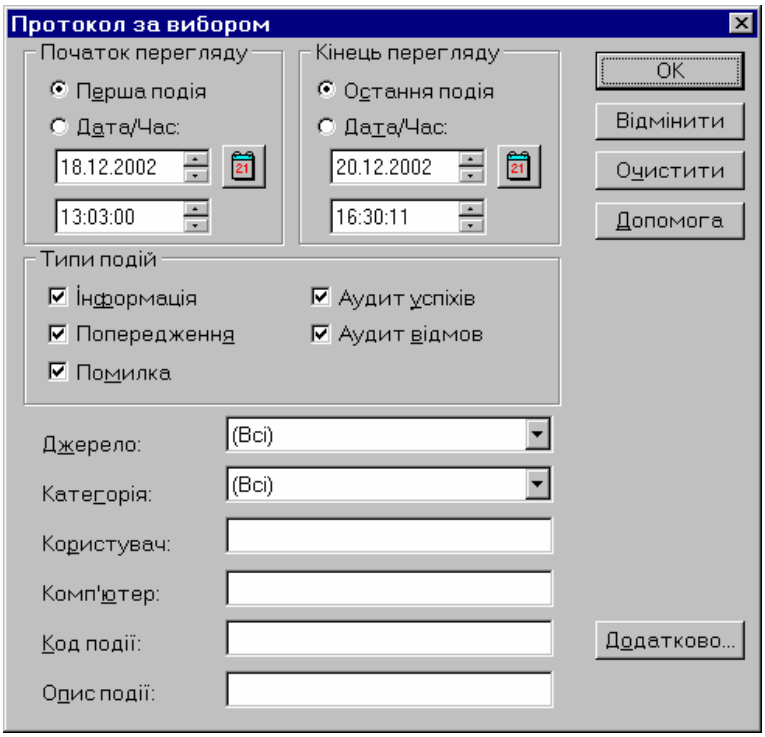

Рисунок 2.7 – Діалогове вікно для формування умов відбору для протоколу за вибором

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

Якщо умови відбору не вказати, до протоколу буде включено всі події, що містяться в журналі, з повним описом подій.

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
	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 – Параметри журналу	Встановлення параметрів журналу реєстрації
	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
Конфігурація – Параметри комп’ютера	Реєстрація подій – Політика аудита	Встановлення політики аудита
	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

Меню	Підменю	Дія
	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
Конфігурація – Встановлення значення за умовчанням		Встановлення значення за умовчанням для параметрів конфігурації
Настройка	Панелі інструментів	Настройка панелі інструментів
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).

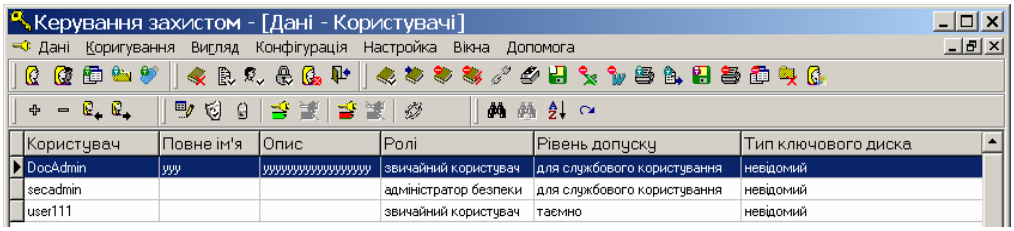

Рисунок 3.1 – Вікно для роботи з даними про користувачів

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 – Експортувати перелік користувачів		Експорт переліку користувачів для ототожнення на інших комп’ютерах та створення резервних копій бази облікових записів
Коригування – Імпортувати перелік користувачів		Імпорт переліку користувачів з резервного носія для проведення відновлення бази облікових записів
Коригування – Змінити пароль		Зміна пароля користувача
Коригування – Ототожнити користувача		Ототожнення користувача з одного комп’ютера на іншому

Пункт меню	Кнопка	Дія
Вигляд – Пошук		Пошук користувача за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортування даних		Сортування даних за вказаними полями
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 (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).

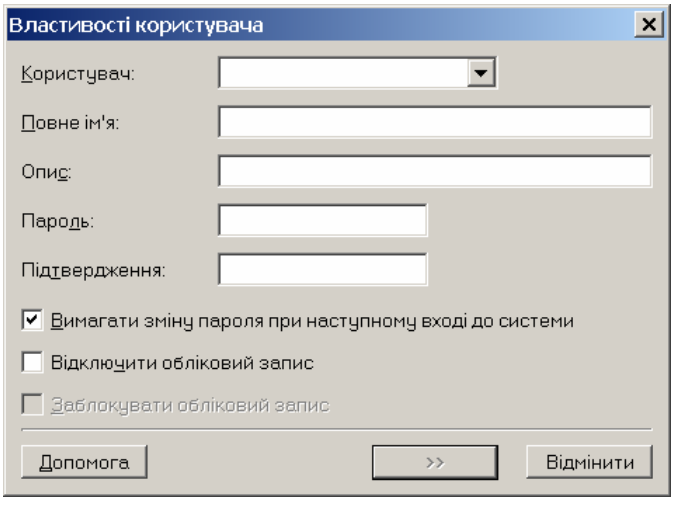

Рисунок 3.2 – Діалогове вікно для введення імені та властивостей нового користувача

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).

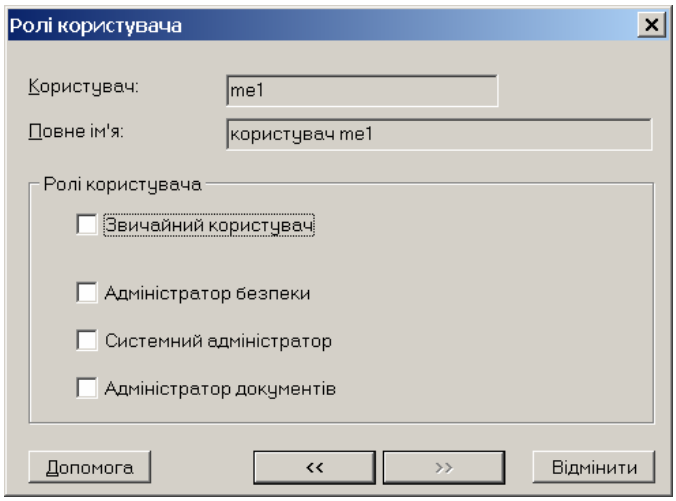

Рисунок 3.3 – Діалогове вікно для введення ролей нового користувача

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).

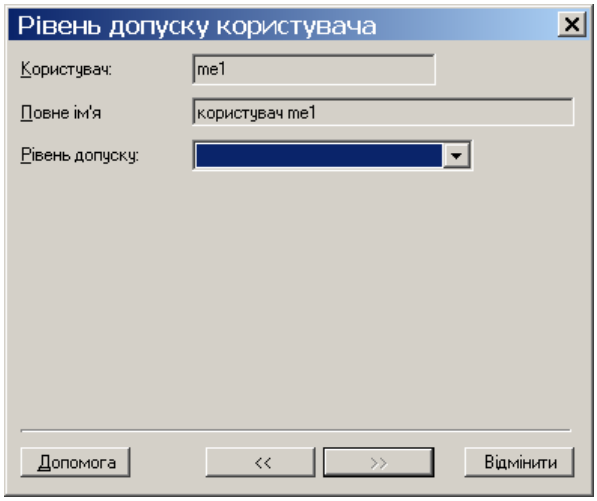

Рисунок 3.4 – Діалогове вікно для введення рівня допуску нового користувача

У полі *Рівень допуску* вводиться рівень допуску користувача. При цьому вибирається одне із запропонованих значень:

– цілком таємно;
– таємно;
– для службового користування;
– відкрита інформація.

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).

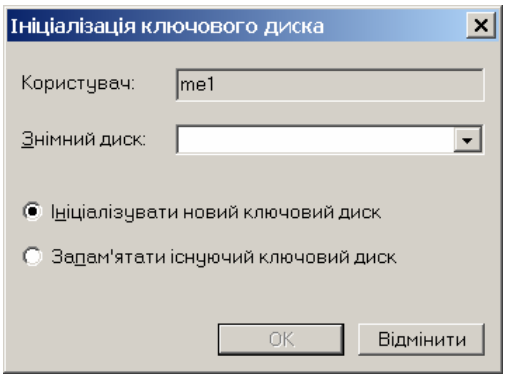

Рисунок 3.5 – Вікно для ініціалізації ключового диска

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  . 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 *K1* та *K2* під іменем *User1*. Нижче описаний процес встановлення ототожнення.

1) На комп'ютері *K1* 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 *K1_Users.cds*.

2) На комп'ютері *K2* за допомогою пункту меню *БД захисту – Користувачі* відкрити перелік користувачів.

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

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

– у діалозі вказати файл *K1_Users.cds*;

– обрати в переліку рядок *K1\User1*;

– зберегти ототожнення.

4) Повторити кроки 1) – 3) для встановлення ототожнення „у зворотному напрямку" (тобто виконати експорт переліку користувачів на комп'ютері *K2* та встановити ототожнення на комп'ютері *K1*).

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).

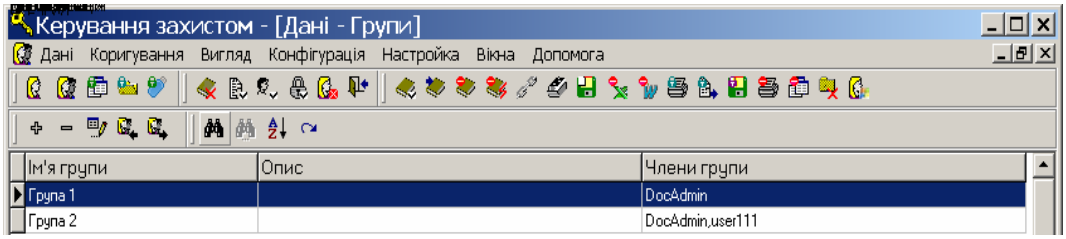

Рисунок 3.6 – Вікно для роботи з даними про групи користувачів

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 – Експортувати перелік груп користувачів		Експорт переліку груп користувачів для створення резервних копій бази облікових записів
Коригування – Імпортувати перелік груп користувачів		Імпорт переліку користувачів з резервного носія для проведення відновлення бази облікових записів
Вигляд – Пошук		Пошук групи за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за вказаними полями
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).

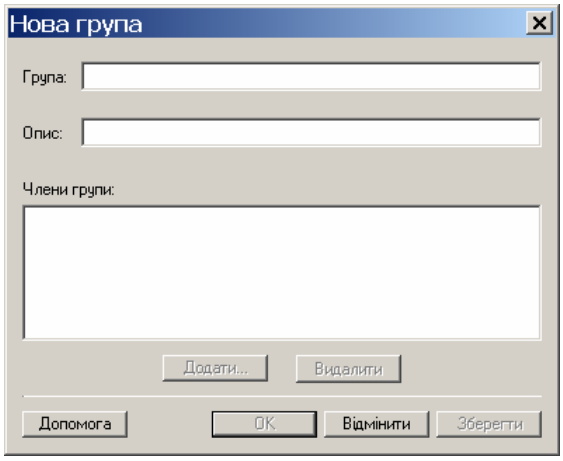

Рисунок 3.7 – Діалогове вікно для введення нової групи користувачів

За допомогою кнопки *Додати* можна включити до групи одного або декількох нових членів. Для цього призначене діалогове вікно *Користувачі* (рисунок 3.8).

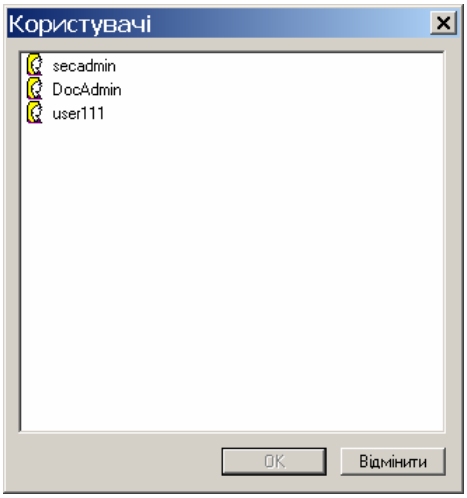

Рисунок 3.8 – Діалогове вікно для включення до групи нового члена

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 . Коригування відбувається за правилами, наведеними в п. 3.2.2.1.

3.2.3 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 файла. У головному меню додатково з'являються пункти *Коригування* та *Вигляд*. Робота з даними про захищені процеси проводиться у вікні *Дані – Захищені процеси* (рисунок 3.9).

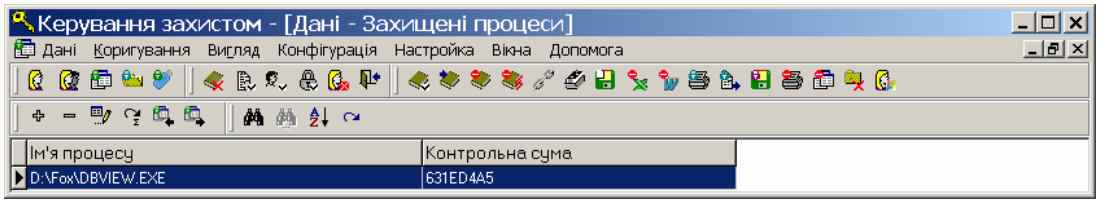

Рисунок 3.9 – Вікно для роботи з даними про захищені процеси

Можливості, які надає програма при роботі з даними про захищені процеси, наведено в таблиці 3.4.

Таблиця 3.4

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 файла
Коригування – Експортувати перелік захищених процесів		Експорт переліку захищених процесів для створення резервних копій
Коригування – Імпортувати перелік захищених процесів		Імпорт переліку захищених процесів з резервного носія для проведення відновлення
Вигляд – Пошук		Пошук захищеного процесу за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за вказаними полями
Вигляд – Поновити дані		Поновлення даних про захищені процеси

3.2.3.1 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 3.10).

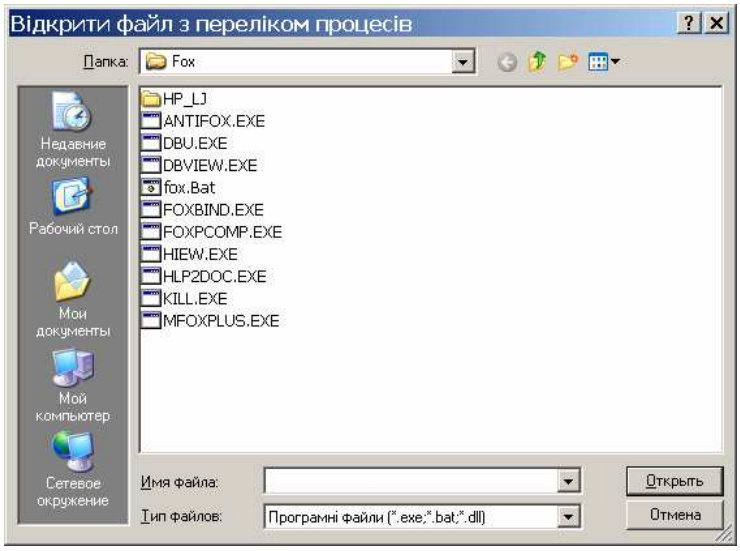

Рисунок 3.10 – Діалогове вікно для введення імені нового захищеного процесу

Після натискання кнопки *Открыть* з'являється діалогове вікно для введення даних про захищений процес – списку доступу та списку аудита (рисунок 3.11).

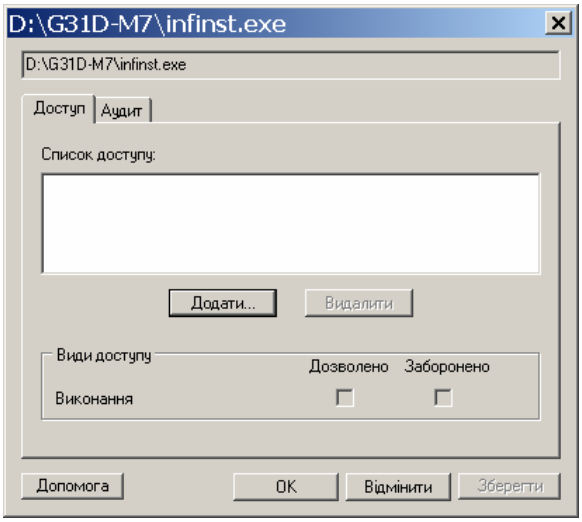

Рисунок 3.11 – Діалогове вікно для введення списку доступу захищеного процесу

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 3.12).

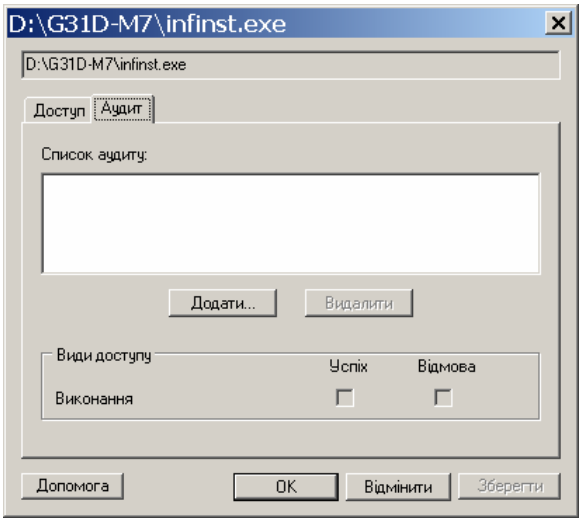

Рисунок 3.12 – Діалогове вікно для введення списку аудиту захищеного процесу

За допомогою кнопки *Додати* можна додати користувача чи групу користувачів до списку аудита цього процесу. Відмітка у полі *Успіх* означає 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.

3.2.3.2 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.

3.2.3.3 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 . Коригування відбувається за правилами, наведеними в п. 3.2.3.1.

3.2.4 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 признак, що вказує на наявність переліку 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 3.13).

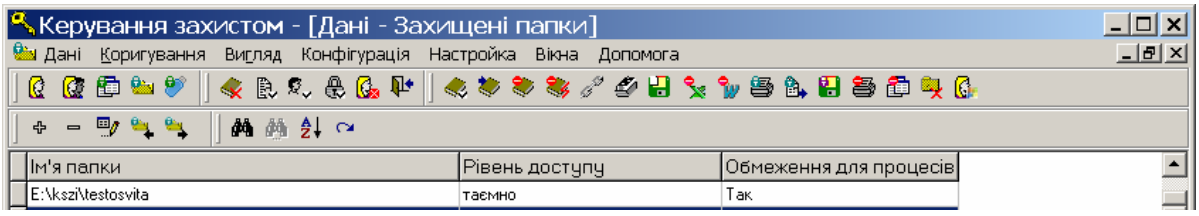

Рисунок 3.13 – Вікно для роботи з даними про захищені папки

Можливості, які надає програма під час роботи з даними про захищені папки, наведено в таблиці 3.5.

Таблиця 3.5

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 – Експортувати перелік захищених папок		Експорт переліку захищених папок для створення резервних копій переліку захищених папок
Коригування – Імпортувати перелік захищених папок		Імпорт переліку захищених папок з резервного носія для проведення відновлення переліку захищених папок
Вигляд – Пошук		Пошук захищеної папки за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за вказаними полями
Вигляд – Поновити дані		Поновлення даних про захищені папки

3.2.4.1 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 3.14).

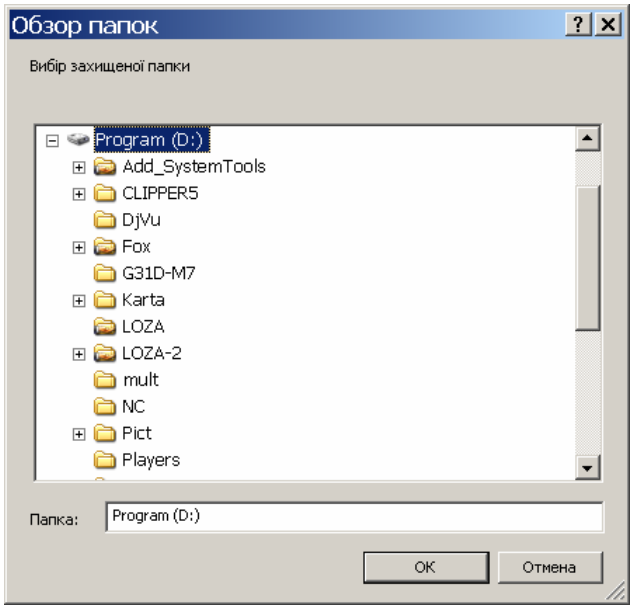

Рисунок 3.14 – Діалогове вікно для введення імені нової захищеної папки

Після натискання кнопки *OK* з'являється діалогове вікно для введення даних про захищену папку – загальних параметрів, списку доступу та списку аудита (рисунок 3.15).

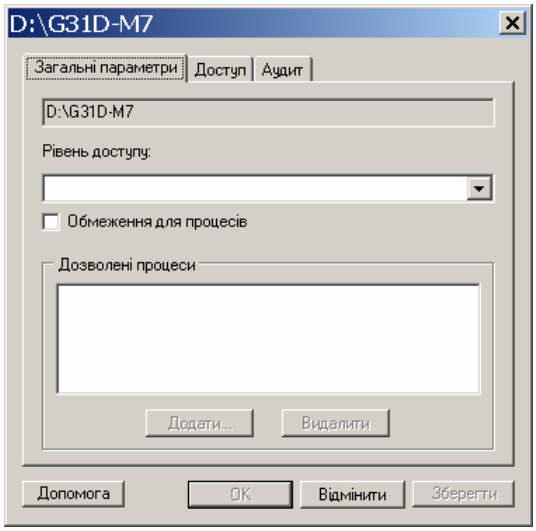

Рисунок 3.15 – Діалогове вікно для введення загальних параметрів для захищеної папки

У полі *Рівень доступу* вводиться рівень доступу папки – максимальний рівень доступу інформації, яка може зберігатись в цій папці. При цьому вибирається одне із запропонованих значень:

- цілком таємно;
- таємно;
- для службового користування;
- відкрита інформація.

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 3.16).

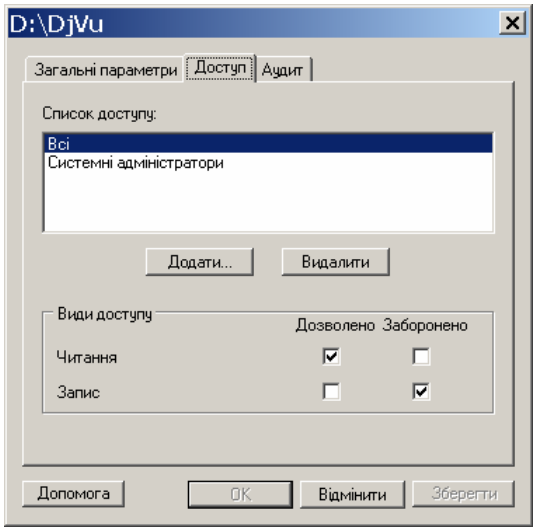

Рисунок 3.16 – Діалогове вікно для введення списку доступу захищеної папки

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 3.17).

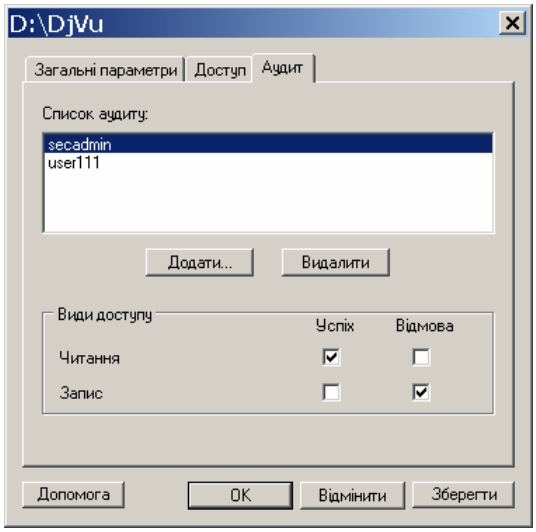

Рисунок 3.17 – Діалогове вікно для введення списку аудиту захищеної папки

За допомогою кнопки *Додати* можна додати користувача чи групу користувачів до списку аудита 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.

3.2.4.2 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.

3.2.4.3 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 . Коригування відбувається за правилами, наведеними в п. 3.2.4.1.

3.2.5 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 признак, що вказує на наявність переліку 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 3.18).

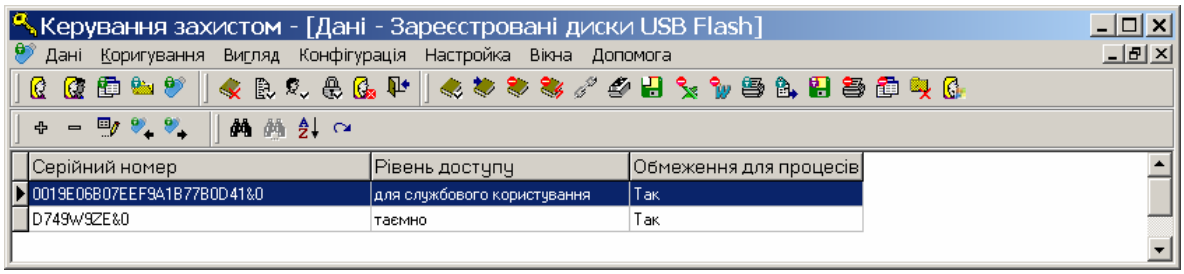

Рисунок 3.18 – Вікно для роботи з даними про зареєстровані диски USB Flash

Можливості, які надає програма під час роботи з даними про зареєстровані диски USB Flash, наведено в таблиці 3.6.

Таблиця 3.6

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 – Експортувати перелік знімних дисків		Експорт переліку зареєстрованих дисків USB Flash для створення резервних копій переліку

Пункт меню	Кнопка	Дія
		зареєстрованих дисків USB Flash
Коригування – Імпортувати перелік знімних дисків		Імпорт переліку зареєстрованих дисків USB Flash з резервного носія для проведення відновлення переліку зареєстрованих дисків USB Flash
Вигляд – Пошук		Пошук зареєстрованого диску USB Flash за вказаними умовами
Вигляд – Продовжити пошук		Продовження початого пошуку
Вигляд – Сортувати дані		Сортування даних за вказаними полями
Вигляд – Поновити дані		Поновлення даних про зареєстровані диски USB Flash

3.2.5.1 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 3.19).

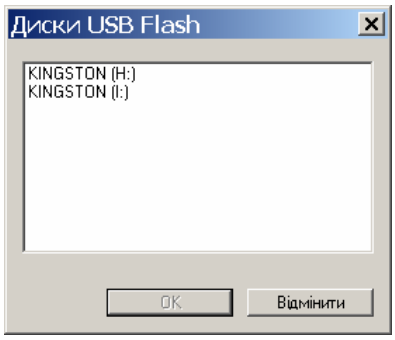

Рисунок 3.19 – Діалогове вікно для вибору знімного диска

Після натискання кнопки *ОК* з’являється діалогове вікно для введення даних про диск – загальних параметрів, списку доступу та списку аудита (рисунок 3.20).

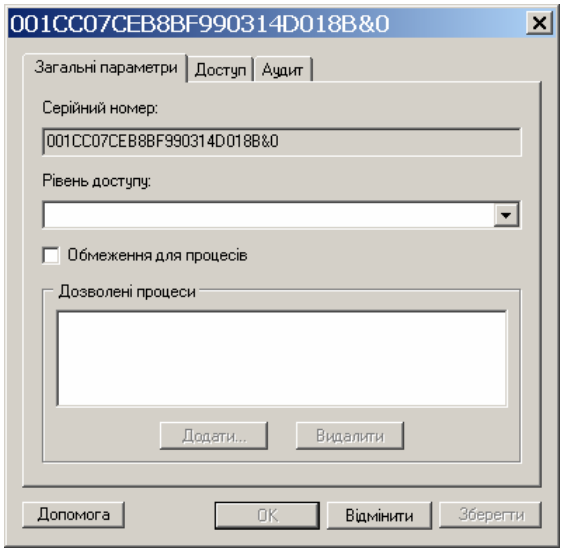

Рисунок 3.20 – Діалогове вікно для введення загальних параметрів для диска

У полі *Рівень доступу* вводиться рівень доступу диска – максимальний рівень доступу інформації, яка може зберігатись на цьому диску. При цьому вибирається одне із запропонованих значень:

- цілком таємно;
- таємно;
- для службового користування;
- відкрита інформація.

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 3.21).

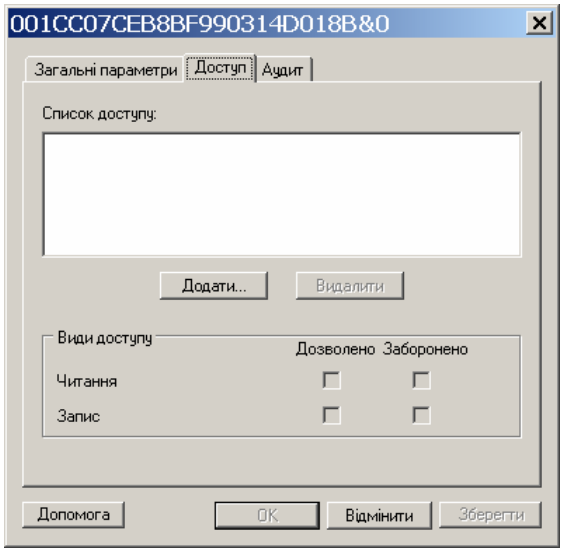

Рисунок 3.21 – Діалогове вікно для введення списку доступу диска

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 3.22).

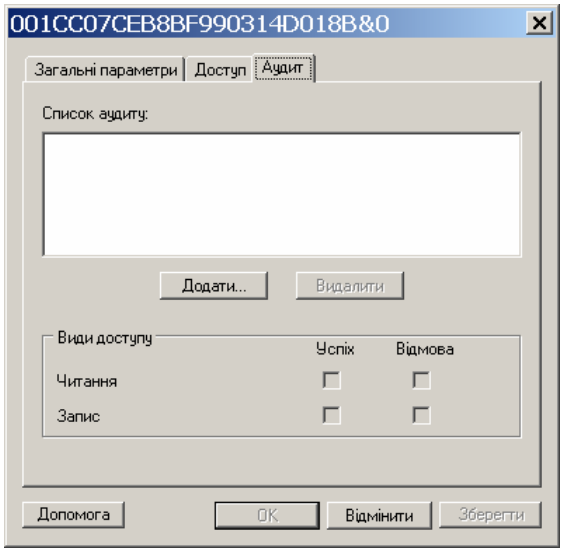

Рисунок 3.22 – Діалогове вікно для введення списку аудиту диска

За допомогою кнопки *Додати* можна додати користувача чи групу користувачів до списку аудита 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.

3.2.5.2 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.

3.2.5.3 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  . Коригування відбувається за правилами, наведеними в п. 3.2.5.1.

3.2.6 Настройка 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”.

3.2.6.1 Встановлення загальних параметрів

3.2.6.1.1 Встановлення параметрів реєстрації подій

3.2.6.1.1.1 Встановлення параметрів журналу захисту

За допомогою пункту меню *Конфігурація – Загальні параметри –Реєстрація подій – Параметри журналу* або кнопки  встановлюються такі параметри конфігурації системи:

- граничний розмір журналу;
- 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 журналу реєстрації подій* (рисунок 3.23).

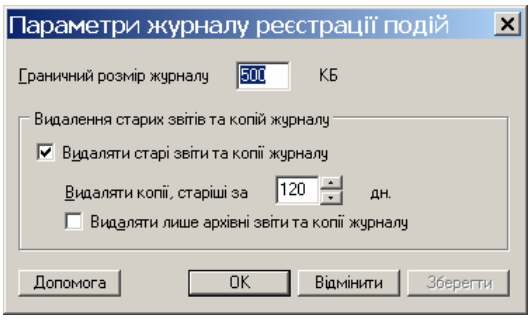

Рисунок 3.23 – Діалогове вікно для встановлення параметрів журналу

У полі *Граничний розмір журналу* визначається граничний розмір журналу реєстрації, після досягнення якого перші події будуть видалятись з 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).

3.2.6.1.2 Встановлення параметрів роботи з документами

3.2.6.1.2.1 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:

- максимальний рівень доступу документів;
- 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.

Для встановлення цих параметрів призначене діалогове вікно *Політика документів* (рисунок 3.24).

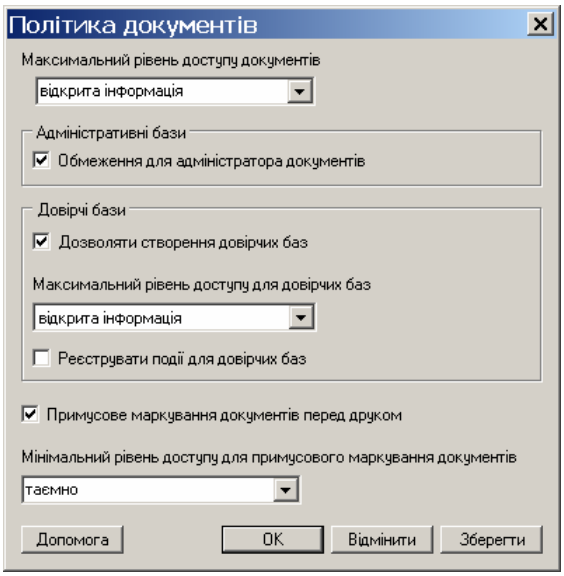

Рисунок 3.24 – Діалогове вікно для встановлення політики документів

У полі *Максимальний рівень доступу документів* вказується максимальний рівень доступу документів, які можуть міститись в базах 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. Значення цього параметра обмежує вибір значення атрибута бази *Максимальний рівень доступу документів*.

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.

3.2.6.1.3 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 3.25).

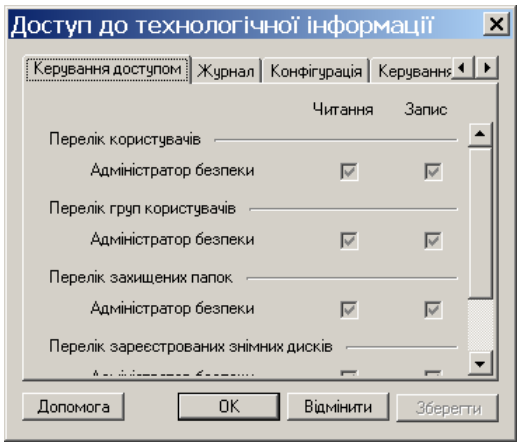

Рисунок 3.25 – Діалогове вікно для встановлення доступів до даних захисту

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).

3.2.6.1.4 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 3.26).

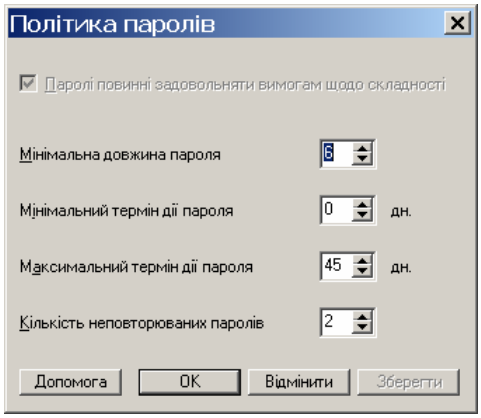

Рисунок 3.26 – Діалогове вікно для встановлення політики паролів

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.

3.2.6.1.5 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 3.27).

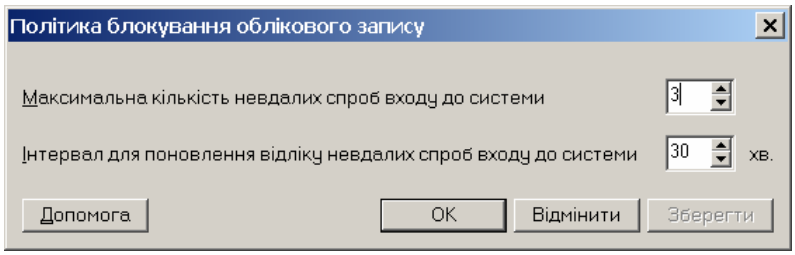

Рисунок 3.27 – Діалогове вікно для встановлення політики блокування облікового запису

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.

3.2.6.1.6 Встановлення параметрів входу до системи

За допомогою пункту меню *Конфігурація – Загальні параметри – Вхід 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 3.28).

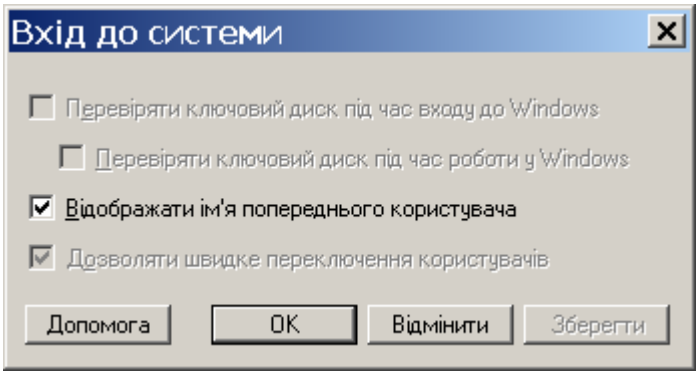

Рисунок 3.28 – Діалогове вікно для встановлення параметрів входу до системи

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 XP він визначає, чи відображається ім'я попереднього користувача в діалозі входу до системи ЛОЗА-1. Для Windows Vista/7 цей параметр визначає, чи відображається на екрані перелік користувачів системи.

3.2.6.2 Встановлення параметрів комп'ютера

3.2.6.2.1 Встановлення параметрів реєстрації подій

3.2.6.2.1.1 Встановлення політики аудита

Політика аудита системи визначається параметром конфігурації системи політика аудита.

Політика аудита 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.);

– *доступ до документів* (читання, коригування, друк документів, коригування атрибутів доступу документів та ін.);

– *доступ до баз документів* (читання бази, створення документів, коригування бази та ін.).

Встановлюється політика аудита за допомогою пункту меню *Конфігурація – Параметри комп'ютера – Реєстрація подій – Політика аудита* або кнопки . Для встановлення політики аудита призначене діалогове вікно *Політика аудита* (рисунок 3.29).

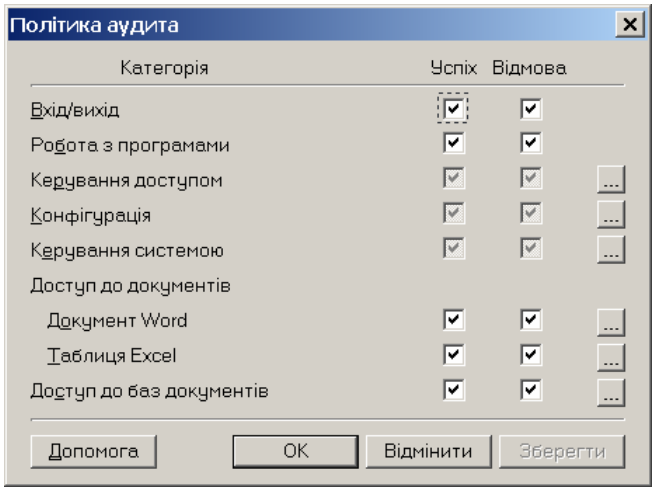

Рисунок 3.29 – Діалогове вікно для настройки політики аудита

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.

Для подій доступу до документів аудит може бути встановлений для різних типів документа (документ Word або таблиця Excel) та рівнів доступу документа, а для подій доступу до баз документів – у залежності від максимального рівня доступу бази. Аудит доступу до документів та баз документів додатково регулюється списками доступу документів та баз документів.

3.2.6.2.1.2 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 3.30).

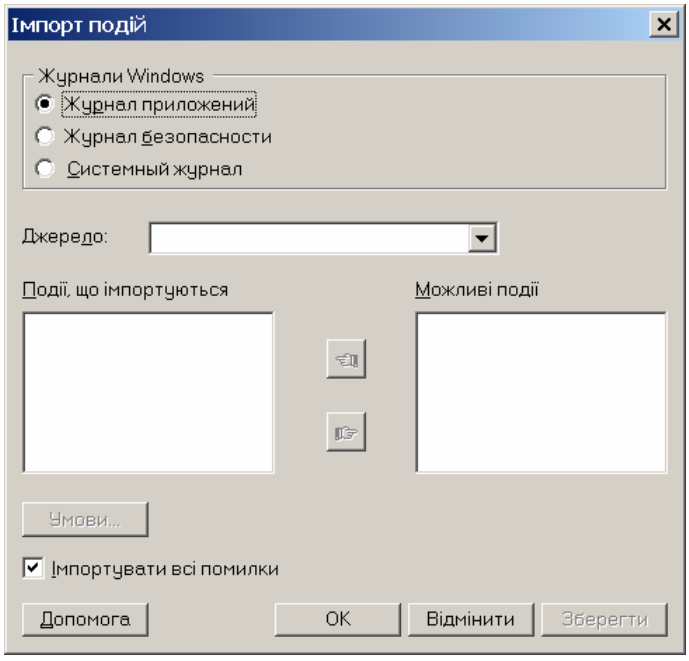

Рисунок 3.30 – Діалогове вікно для встановлення параметрів імпорту подій

Імпорт подій відбувається із трьох журналів Windows – *Журнала приложений*, *Журнала безопасности* та *Системного журнала*. Після вибору в групі *Журнали Windows* одного із цих журналів 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.

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 3.31)

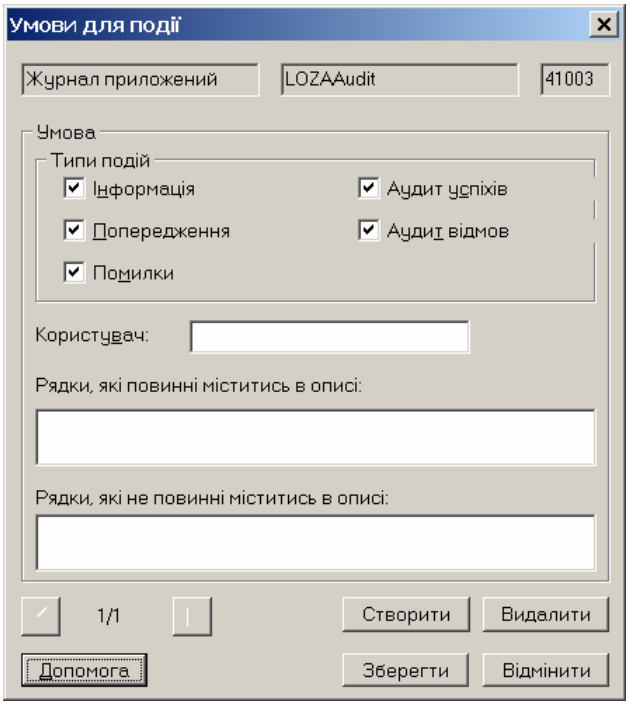

Рисунок 3.31 – Діалогове вікно для встановлення умов для імпорту події

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.

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

3.2.6.2.1.3 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 3.32).

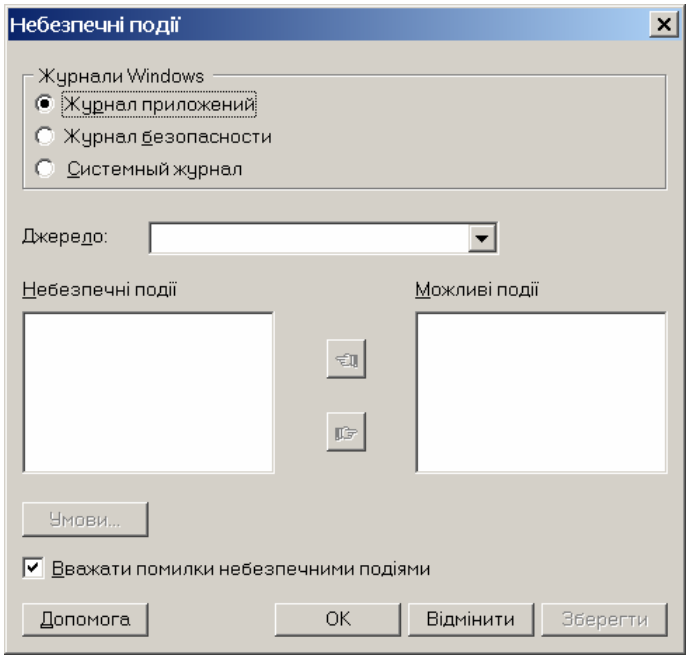

Рисунок 3.32 – Діалогове вікно для визначення небезпечних подій

Робота з переліком небезпечних подій аналогічна роботі з переліком імпортованих подій (п. 3.2.6.2.1.2).

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.

3.2.6.2.1.4 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 3.33).

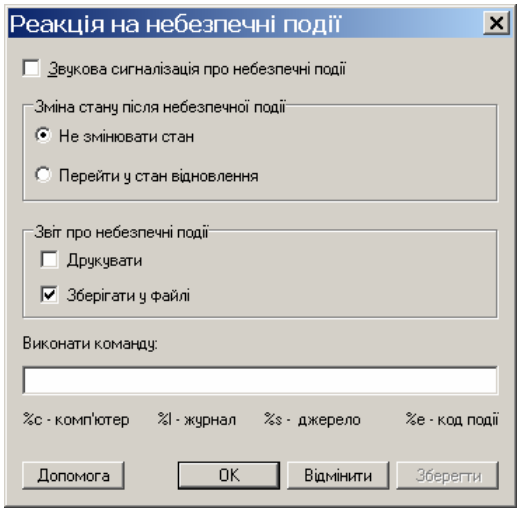

Рисунок 3.33 – Діалогове вікно для визначення реакції на небезпечні події

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 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.

3.2.6.2.2 Встановлення параметрів перевірки цілісності

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

3.2.6.2.2.1 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 3.34).

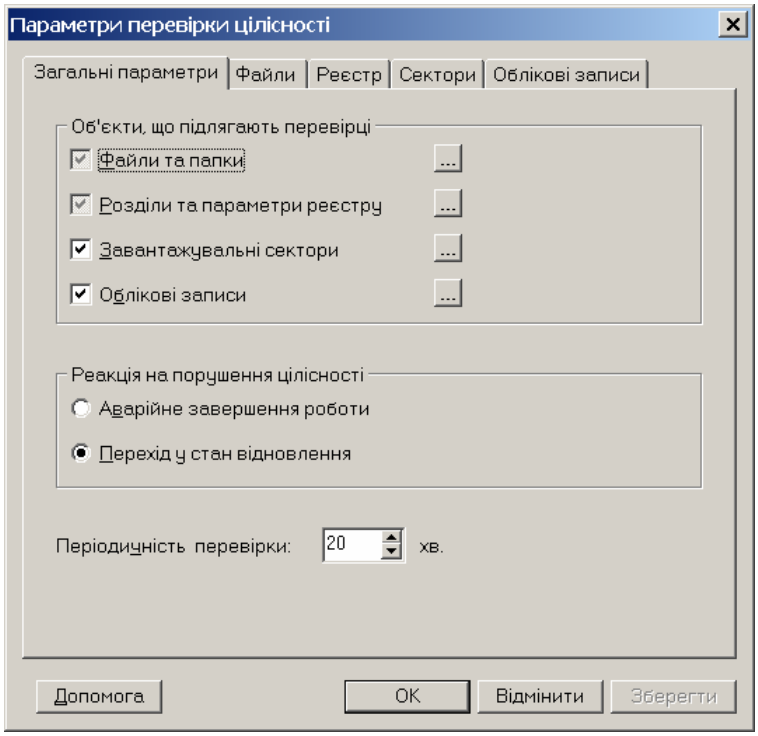

Рисунок 3.34 – Діалогове вікно для встановлення загальних параметрів перевірки цілісності

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.

3.2.6.2.2.2 Перевірка цілісності файлів та папок

3.2.6.2.2.2.1 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 3.35).

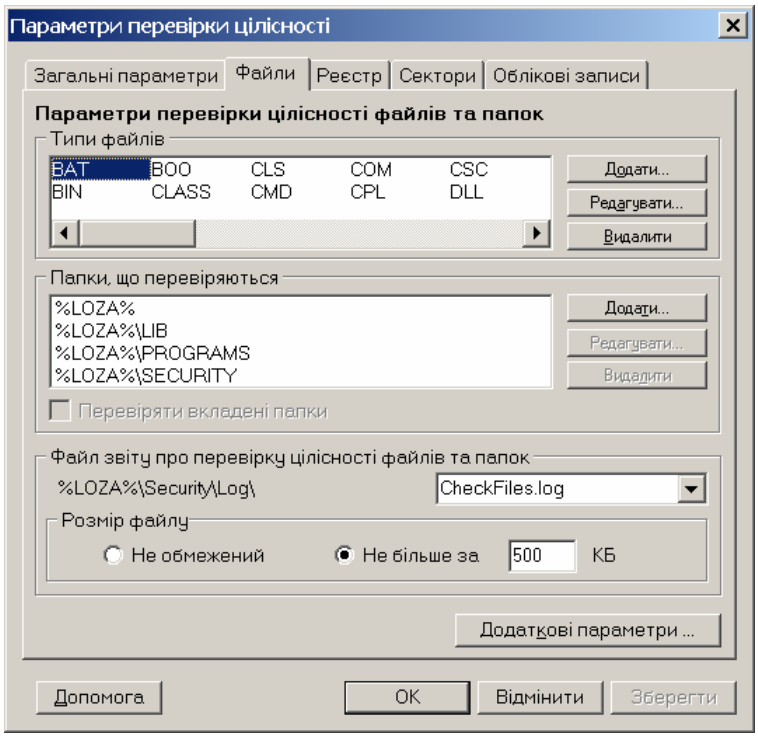

Рисунок 3.35 – Діалогове вікно для встановлення основних параметрів перевірки цілісності файлів та папок

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

3.2.6.2.2.2.1.1 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 3.36).

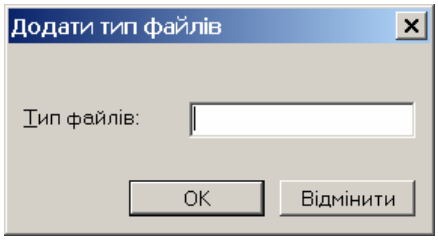

Рисунок 3.36 – Діалогове вікно для введення нового типу файлів до переліку типів файлів

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.

3.2.6.2.2.2.1.2 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 3.37).

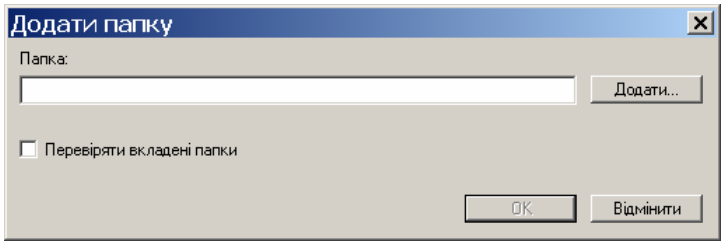

Рисунок 3.37 – Діалогове вікно для введення нової папки

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 3.38).

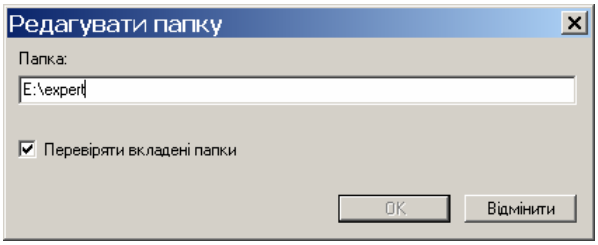

Рисунок 3.38 – Діалогове вікно для редагування імені папки

3.2.6.2.2.2.1.3 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.

3.2.6.2.2.2.2 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 3.39).

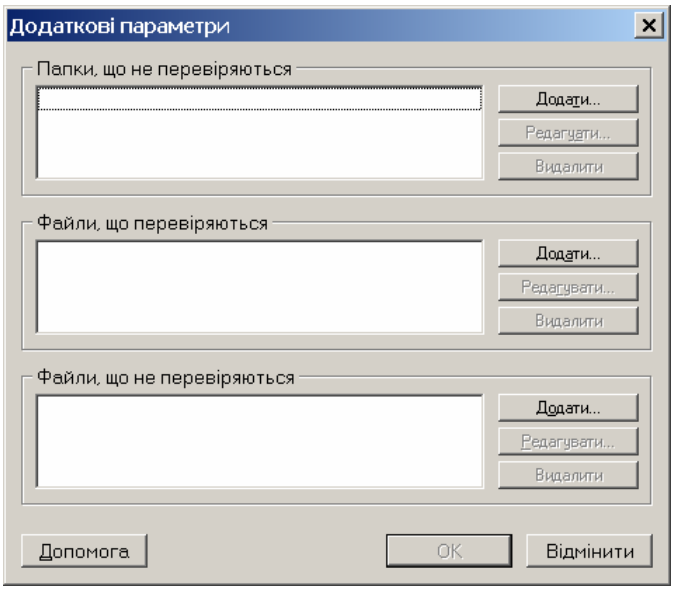

Рисунок 3.39 – Діалогове вікно для встановлення додаткових параметрів перевірки цілісності файлів та папок

3.2.6.2.2.2.2.1 Встановлення переліку папок, що не підлягають перевірці

Встановлення переліку папок відбувається за правилами описаними в п. 3.2.6.2.2.2.1.2.

3.2.6.2.2.2.2.2 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.

3.2.6.2.2.3 Перевірка цілісності розділів та параметрів реєстру

3.2.6.2.2.3.1 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 3.40).

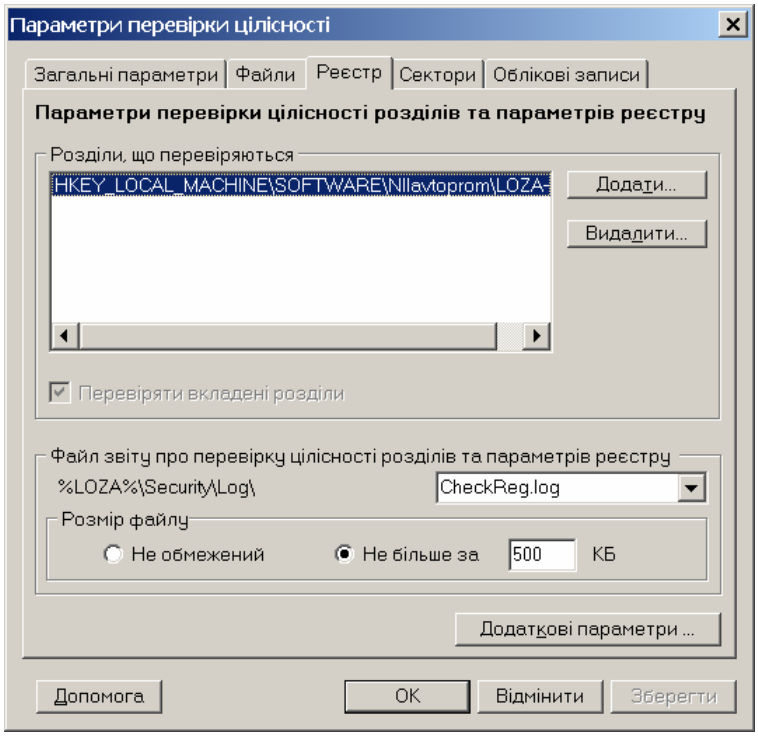

Рисунок 3.40 – Діалогове вікно для встановлення основних параметрів перевірки цілісності розділів та параметрів реєстру

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

3.2.6.2.2.3.1.1 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 3.41).

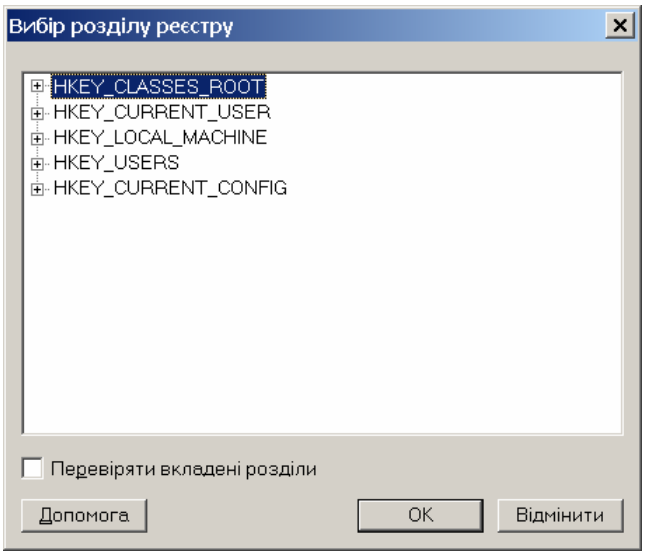

Рисунок 3.42 – Діалогове вікно для включення нового розділу до переліку розділів реєстру

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.

3.2.6.2.2.3.1.2 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.

3.2.6.2.2.3.2 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 3.43).

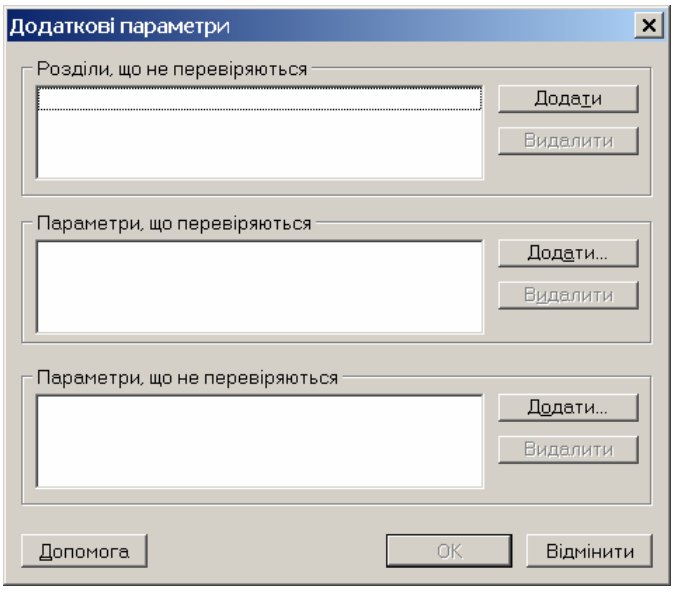

Рисунок 3.43 – Діалогове вікно для встановлення додаткових параметрів перевірки цілісності розділів та параметрів реєстру

3.2.6.2.2.3.2.1 Встановлення переліку розділів реєстру, що не підлягають перевірці

Встановлення переліку розділів реєстру відбувається за правилами, наведеними в п. 3.2.6.2.2.3.1.1.

3.2.6.2.2.3.2.2 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 3.44).

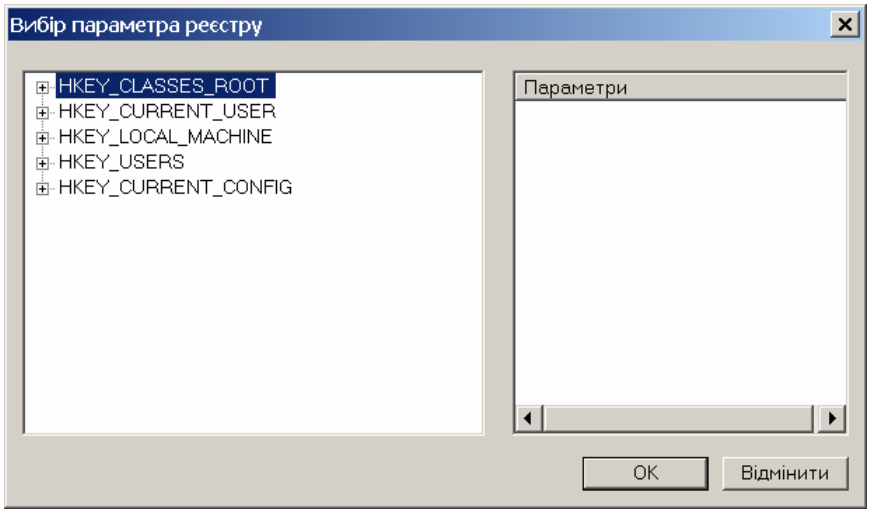

Рисунок 3.44 – Діалогове вікно для введення нового параметра реєстру

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

3.2.6.2.2.4 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 3.45).

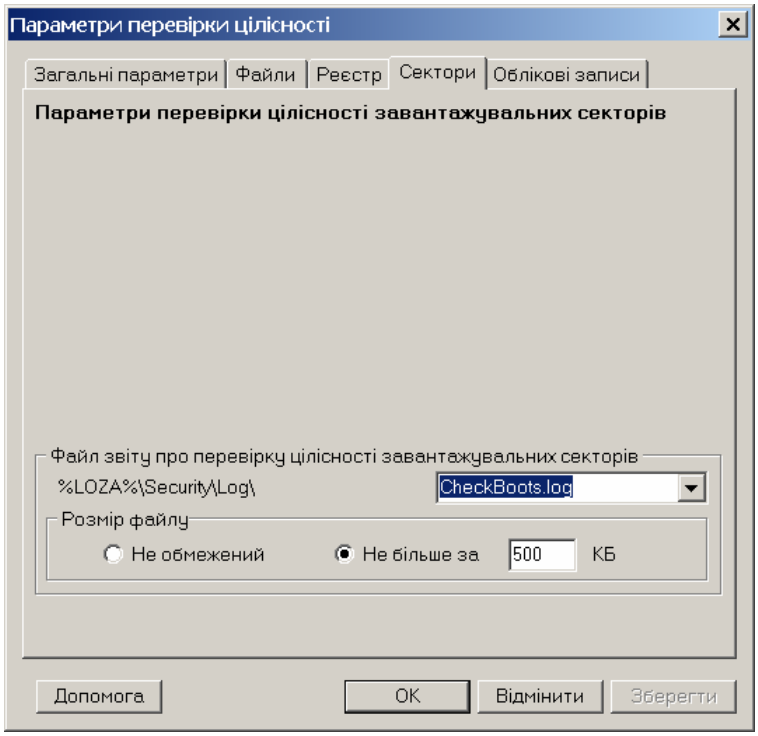

Рисунок 3.45 – Діалогове вікно для встановлення параметрів перевірки цілісності завантажувальних секторів

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.

3.2.6.2.2.5 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 3.46).

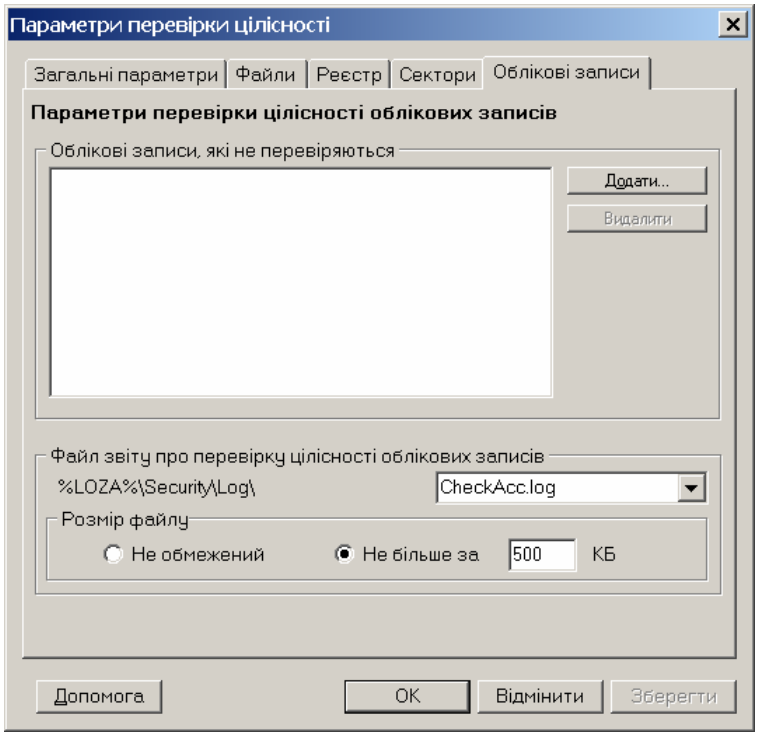

Рисунок 3.46 – Діалогове вікно для встановлення параметрів перевірки цілісності облікових записів

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 3.47).

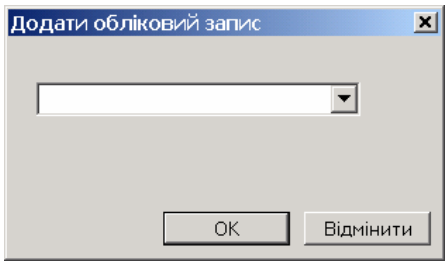

Рисунок 3.47 – Діалогове вікно для введення нового облікового запису

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.

3.2.6.2.3 Встановлення параметрів роботи з документами

3.2.6.2.3.1 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 3.48).

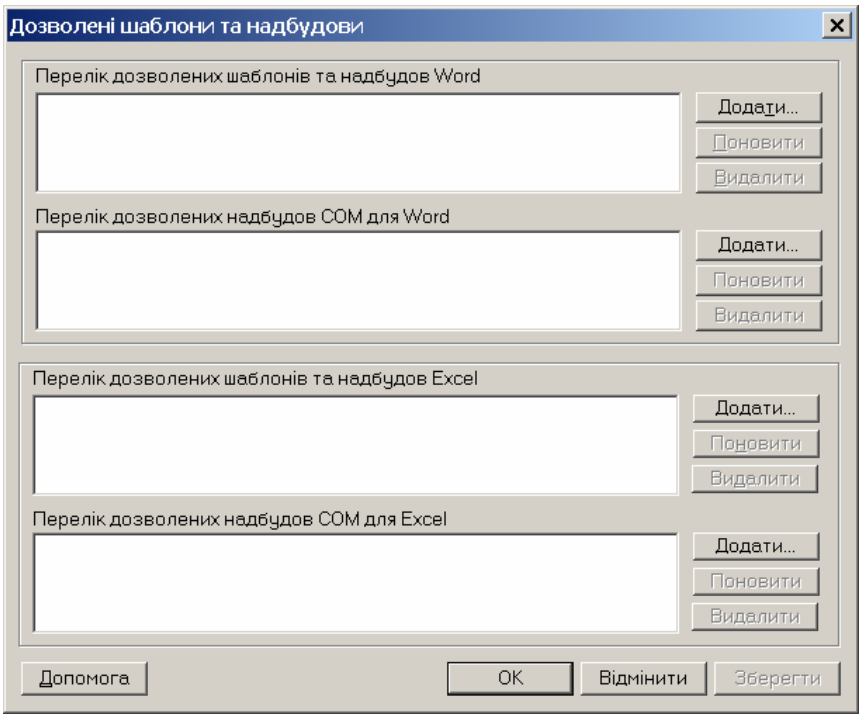

Рисунок 3.48 – Діалогове вікно для встановлення дозволених шаблонів та надбудов

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.

3.2.6.2.3.2 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 3.49).

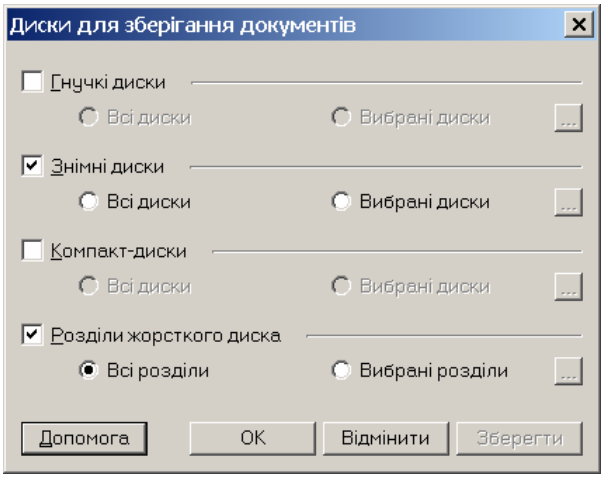

Рисунок 3.49 – Діалогове вікно для встановлення дисків для зберігання документів

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:*).

3.2.6.2.3.3 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 3.50).

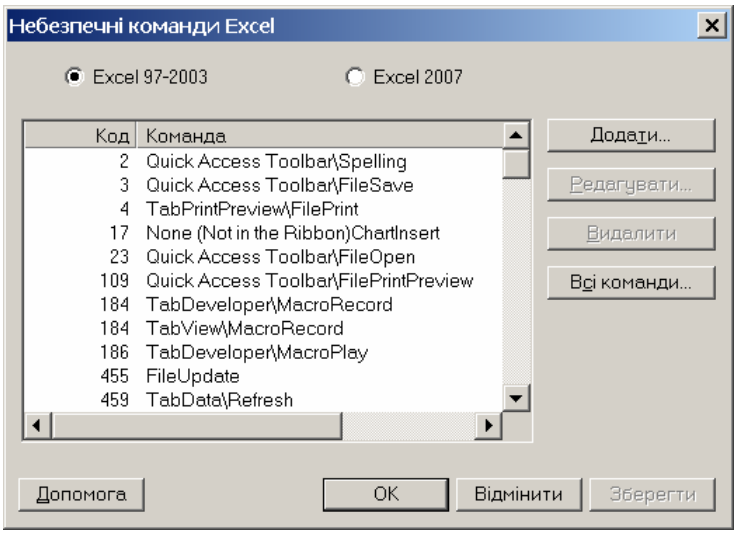

Рисунок 3.50 – Діалогове вікно для встановлення небезпечних команд Excel

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 3.51).

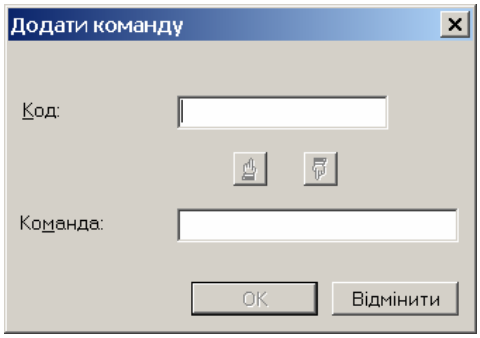

Рисунок 3.51 – Діалогове вікно для введення нової команди до переліку небезпечних команд Excel

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 3.52).

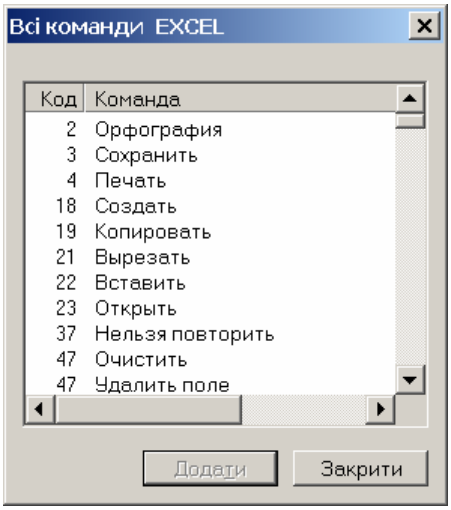

Рисунок 3.52 – Діалогове вікно для введення нових команд до переліку небезпечних команд Excel

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

3.2.6.2.3.4 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 3.53).

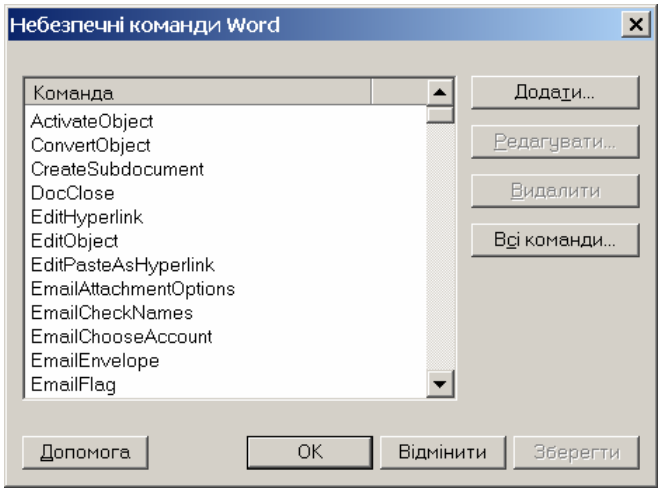

Рисунок 3.53 – Діалогове вікно для встановлення небезпечних команд Word

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 3.54).

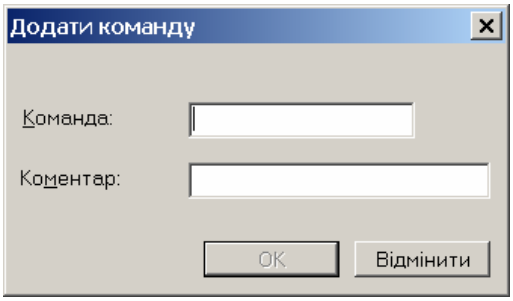

Рисунок 3.54 – Діалогове вікно для введення нової команди до переліку небезпечних команд Word

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 3.55).

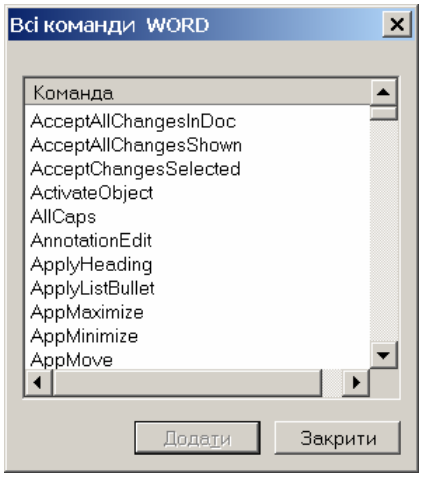

Рисунок 3.55 – Діалогове вікно для введення нових команд до переліку небезпечних команд Word

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

3.2.6.2.3.5 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 3.56).

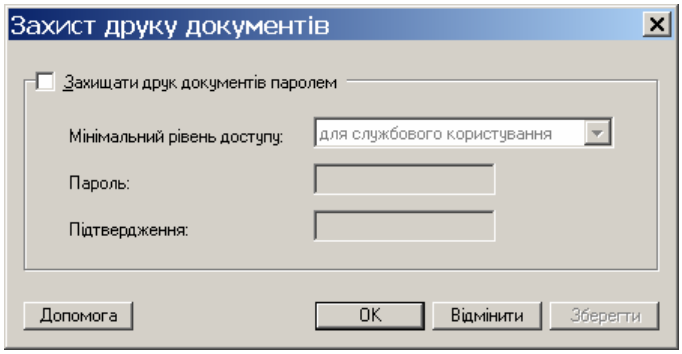

Рисунок 3.56 – Діалогове вікно для встановлення параметрів захисту друку документів

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.

3.2.6.2.3.6 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 3.57).

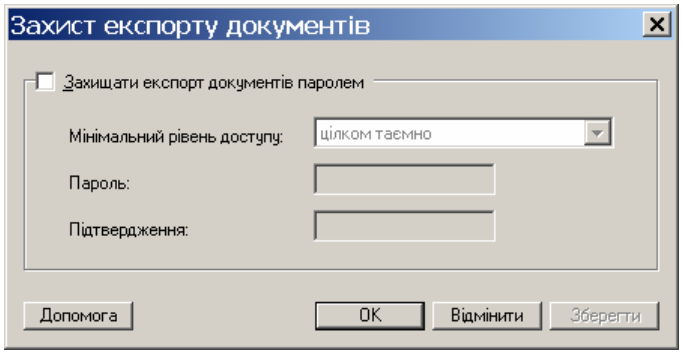

Рисунок 3.57 – Діалогове вікно для встановлення параметрів захисту експорту документів

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.

3.2.6.2.4 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 *Політина знімних дисків* (рисунок 3.58).

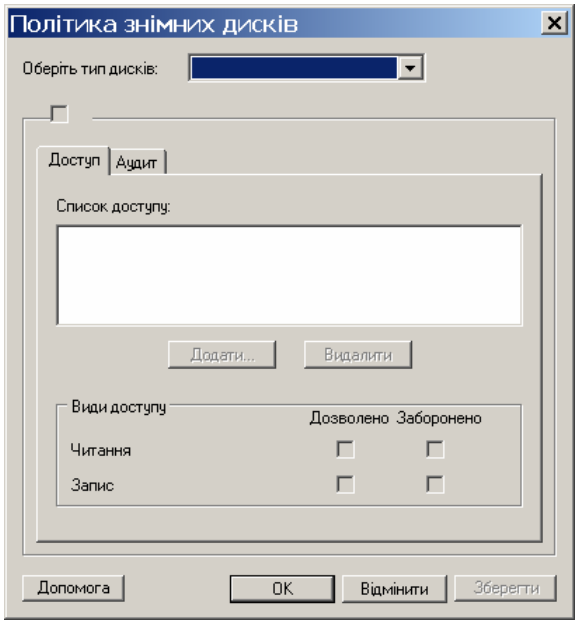

Рисунок 3.58 – Діалогове вікно для встановлення політики знімних дисків

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. 3.2.5.1).

3.2.6.2.5 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 3.59).

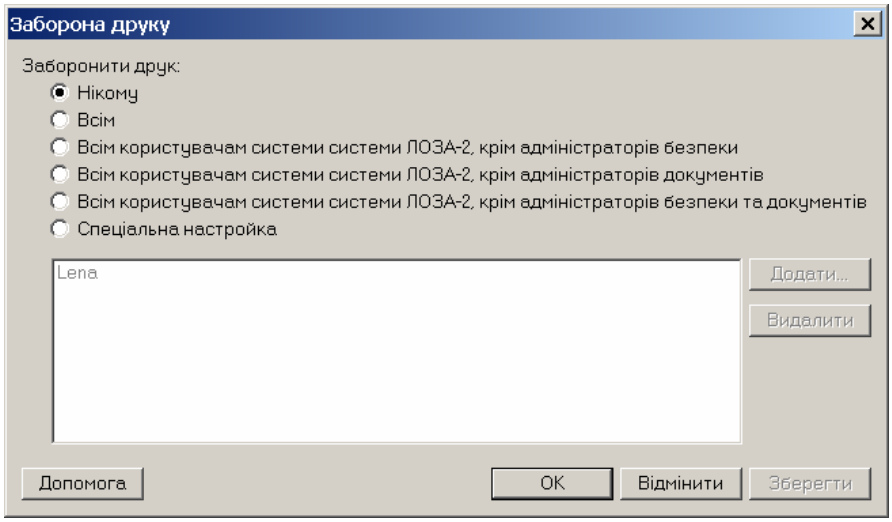

Рисунок 3.59 – Діалогове вікно для встановлення параметрів заборони друку

У разі обрання опції *Спеціальна настройка* 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.

3.2.6.2.6 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 Word, 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 3.60).

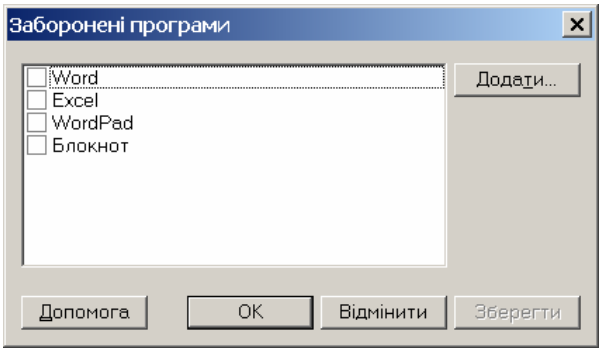

Рисунок 3.60 – Діалогове вікно для встановлення переліку заборонених програм

3.2.6.2.7 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 3.61).

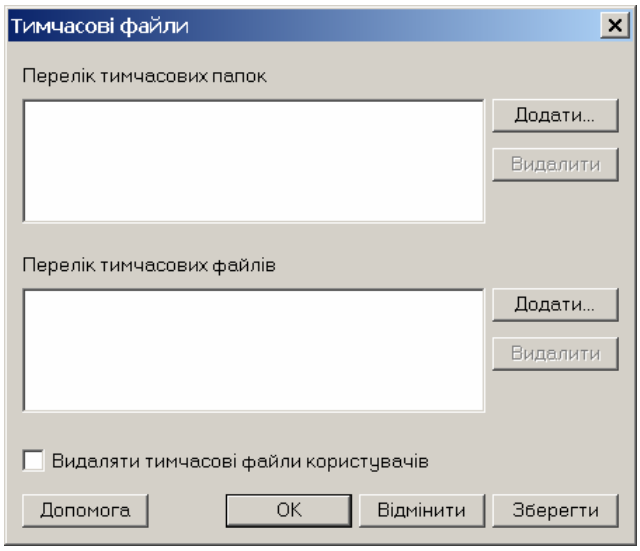

Рисунок 3.61 – Діалогове вікно для встановлення переліку тимчасових файлів

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.

3.2.6.2.8 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 аудита. 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 3.62).

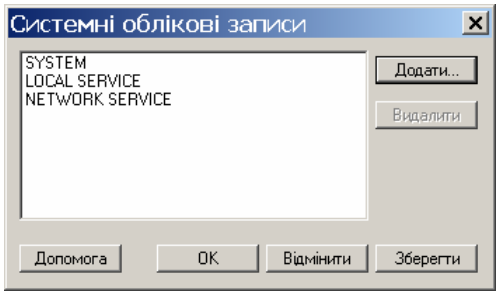

Рисунок 3.62 – Діалогове вікно для встановлення переліку системних облікових записів

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 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 3.63).

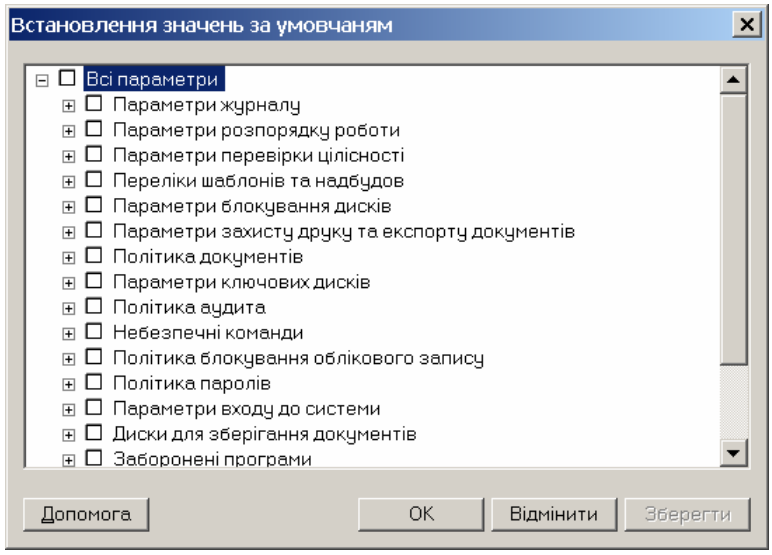

Рисунок 3.63 – Діалогове вікно для встановлення значень за умовчанням для параметрів конфігурації системи

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, наведене на рисунку 4.1.

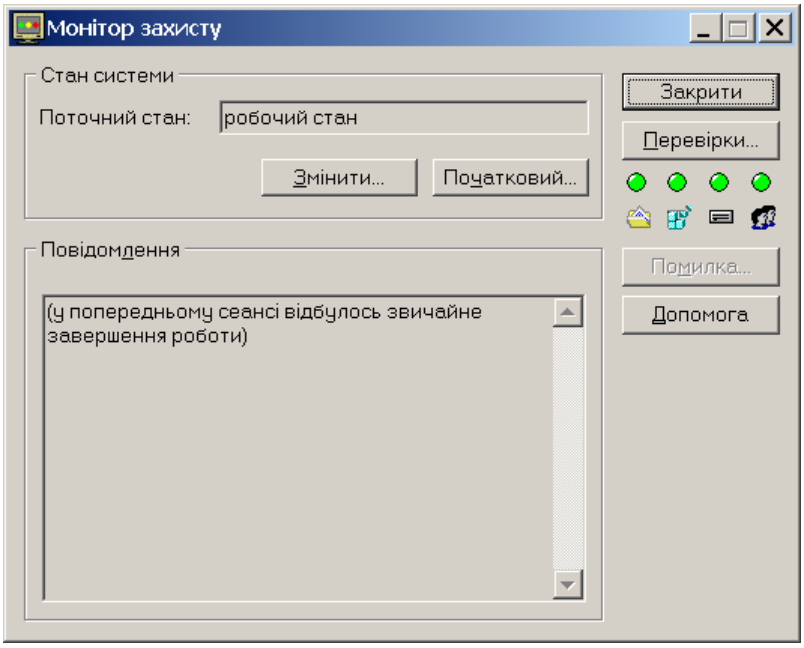

Рисунок 4.1 – Головне вікно програми

У групі *Стан системи* відображається поточний стан автоматизованої системи. Кнопки *Змінити* та *Початковий* дозволяють відповідно змінити поточний стан та встановити початковий стан для наступного сеансу роботи (див п.).

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. На початку роботи, коли здійснюється перехід у початковий стан, назва стану не відображається, оскільки поточний стан не визначений. У той час, коли система виходить із деякого стану, його назва починає блимати.

Кнопка *Змінити* призначена для зміни стану системи вручну. Новий стан необхідно обрати в діалоговому вікні *Зміна стану*, яке зображено на рисунку 4.2.

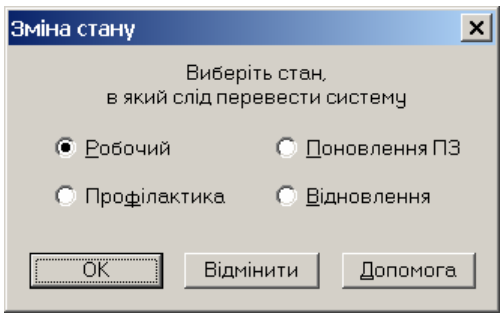

Рисунок 4.2 – Діалогове вікно для вибору стану

Кнопка *Початковий* дозволяє встановити початковий стан для наступного сеансу роботи (для цього використовується аналогічне діалогове вікно).

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).

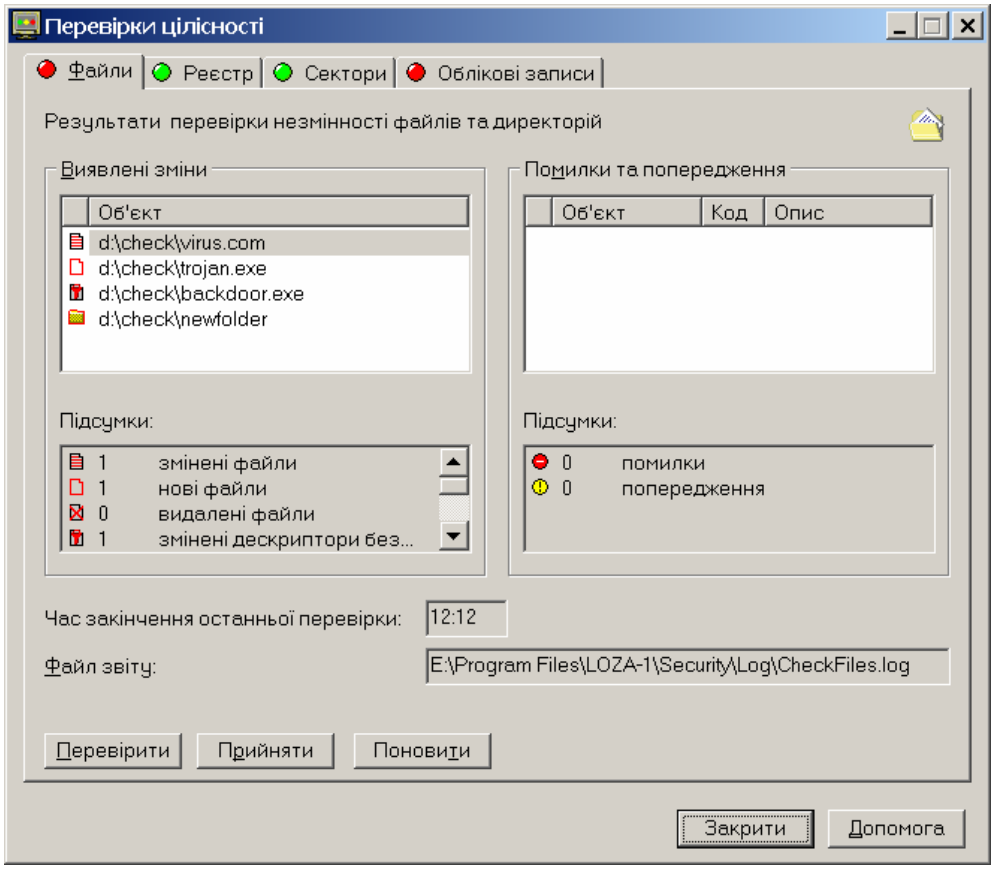

Рисунок 4.3 – Результати перевірки цілісності програмного середовища

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).

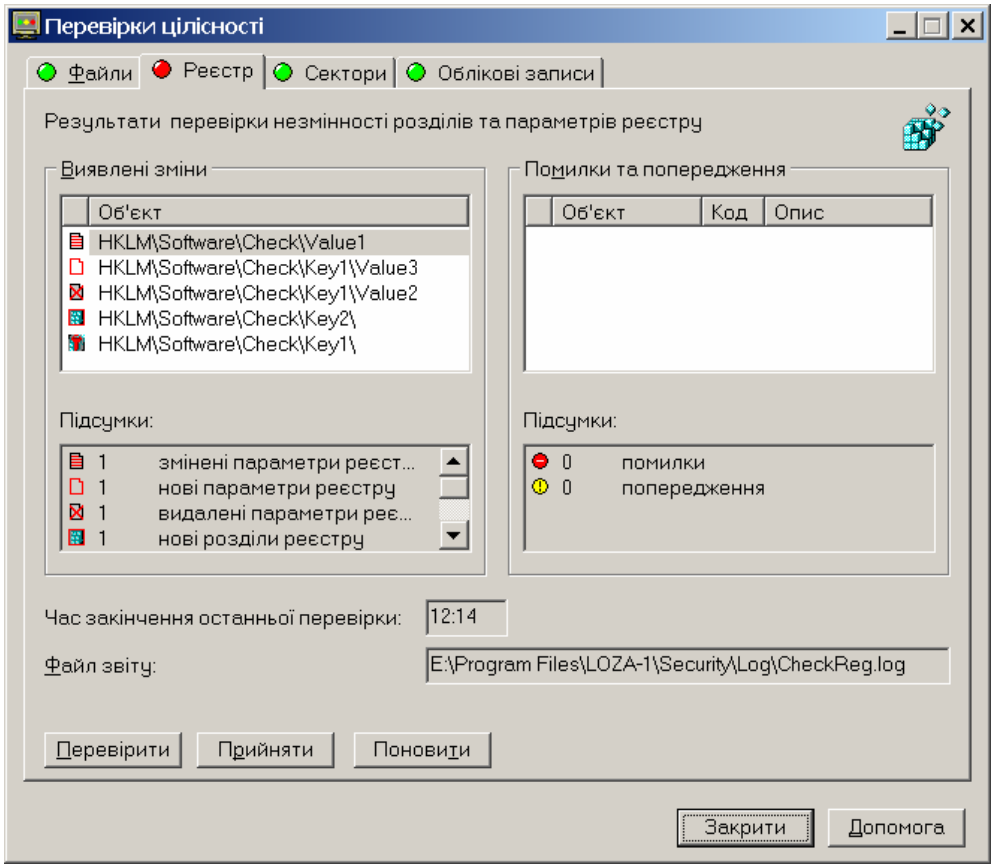

Рисунок 4.4 – Результати перевірки цілісності реєстру

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).

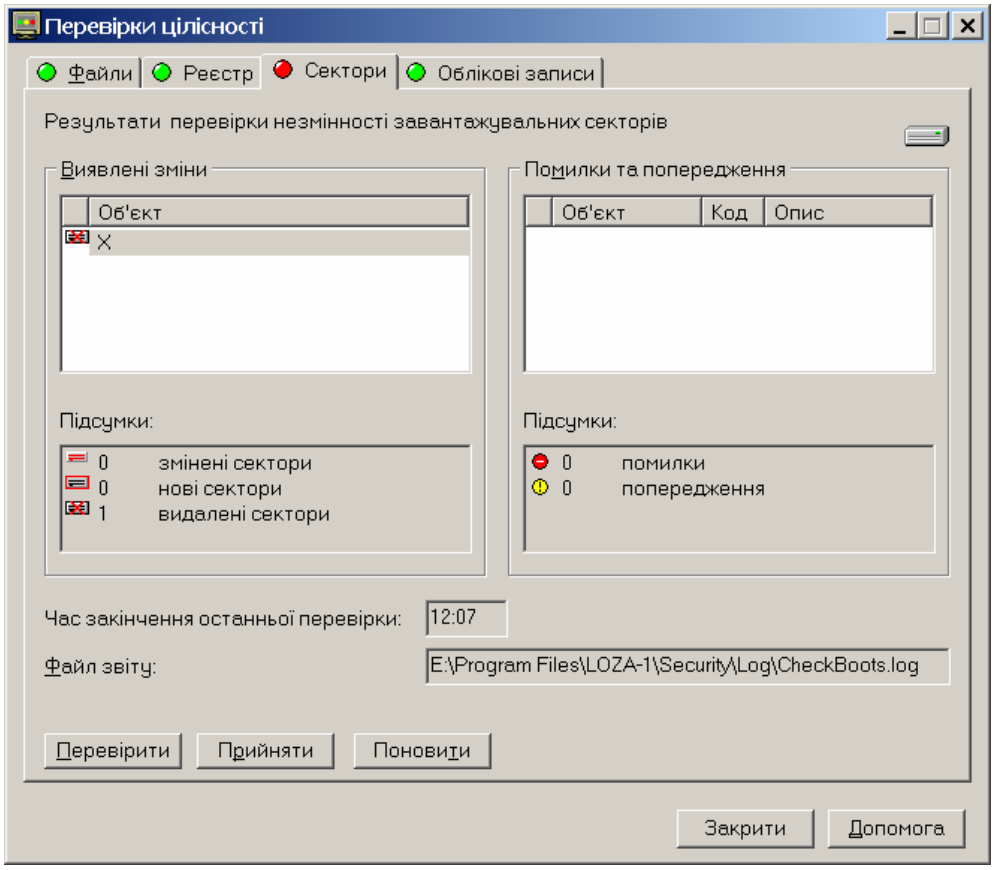

Рисунок 4.5 – Результати перевірки цілісності завантажувальних секторів

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 поновлення ПЗ або в стані відновлення (під час перебування системи в робочому стані та в стані профілактики 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).

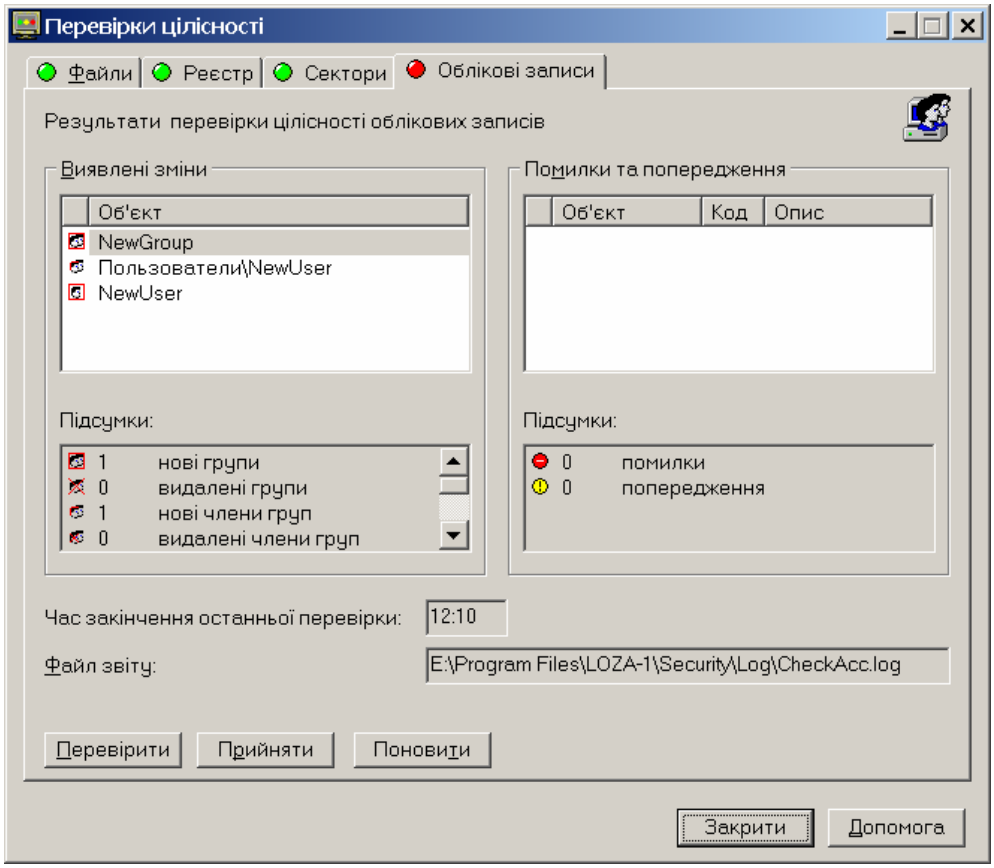

Рисунок 4.6 – Результати перевірки облікових записів

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 поновлення ПЗ або в стані відновлення (під час перебування системи в робочому стані та стані профілактики 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 на рисунку 4.8, і стає доступною кнопка *Помилка*.

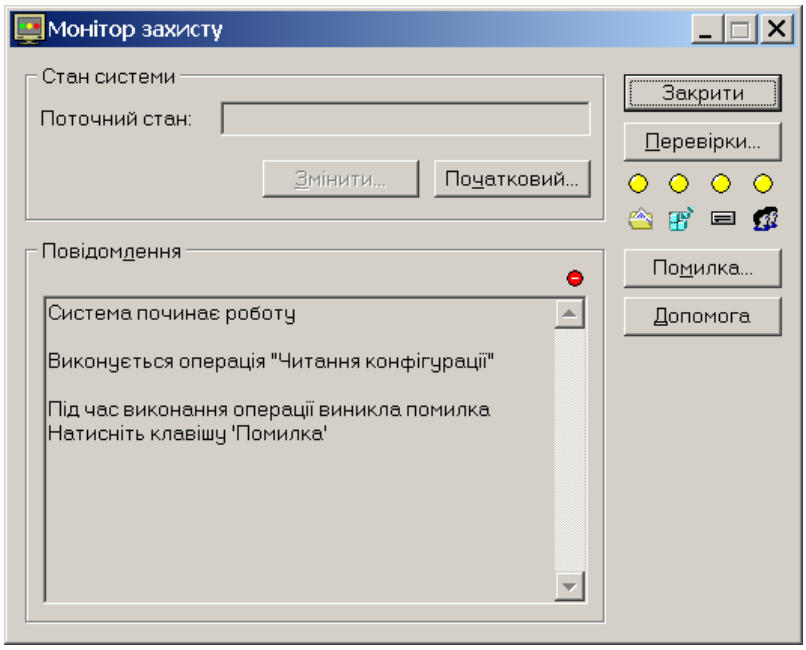

Рисунок 4.8 – Повідомлення про помилку у головному вікні

Після натискання кнопки *Помилка* з’являється вікно, зображене на рисунку 4.9, яке дозволяє обрати спосіб обробки помилки.

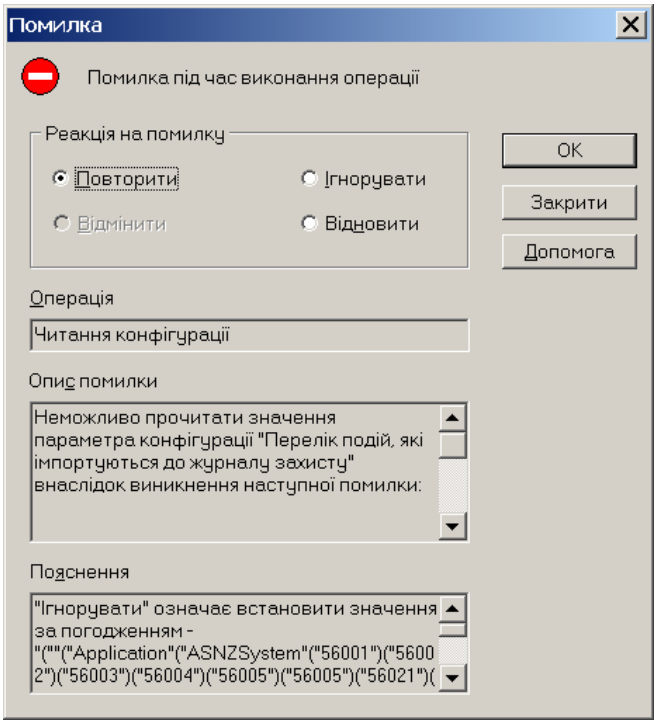

Рисунок 4.9 – Опис помилки

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*, як показано на рисунку 4.9.

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* (див. рис. 5.1), адміністратору може тимчасово дозволити друк, який був заборонений за допомогою параметра конфігурації `спосіб заборони друку` та `облікові записи для заборони друку` (див. п. 3.2.6.2.5). Перед натискання 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 адміністратора вийме свій ключовий диск.

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

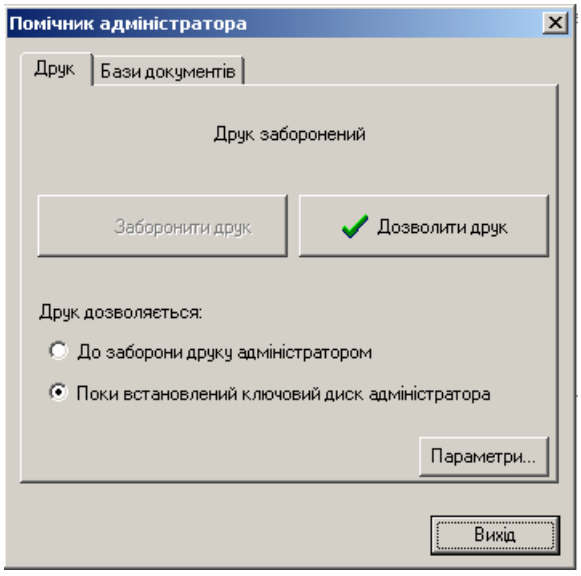

Рисунок 5.1

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. 5.2) 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* (див. рис. 5.2). Перед натискання 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.

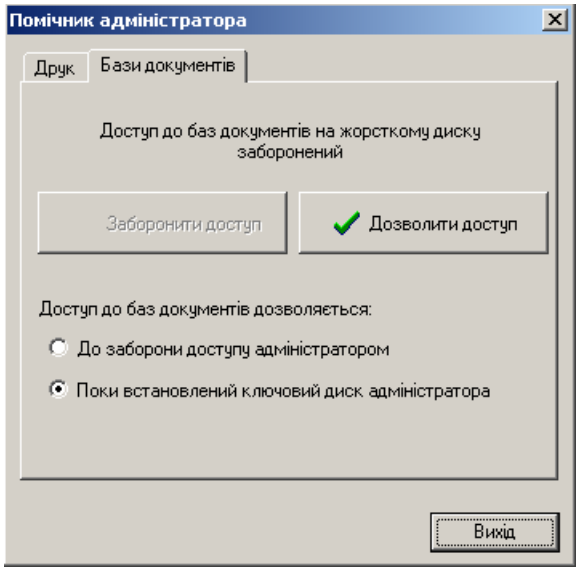

Рисунок 5.2

5.2 Програма *Відновлення пошкодженої бази документів*

Кожна база документів містить декілька службових файлів, пошкодження яких може призвести до неможливості працювати з однією чи декількома папками, або навіть із усією базою. Попри те, що при роботі із службовими файлами в системі ЛОЗА-1 використовуються засоби відмово стійкості, збої програмного чи апаратного забезпечення можуть призвести до пошкодження цих файлів. Для відновлення службових файлів до складу системи ЛОЗА-1 включено програму *Відновлення пошкодженої бази документів* (%LOZA%\LIB\RecoverDamagedBase.exe).

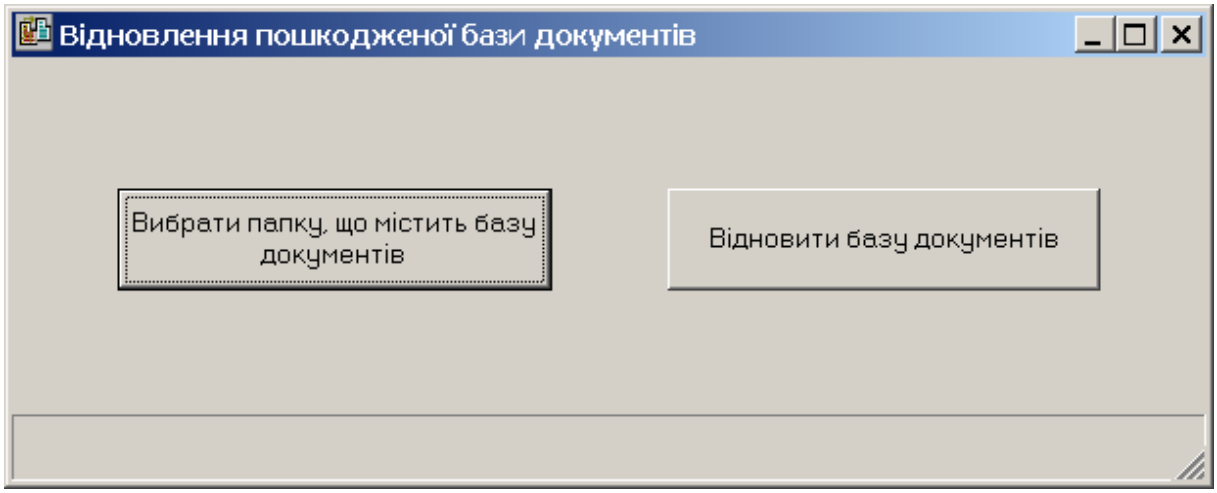

Рисунок 5.1 – Головне вікно програми

Для відновлення за допомогою цієї програми слід виконати описані нижче дії.

1) Перевести систему у стан відновлення.

2) Якщо пошкоджена база зберігається на жорсткому диску, треба за допомогою програми *Помічник адміністратора* (%LOZA%\LIB\AdminAssistant.exe) дозволити доступ до баз документів (на сторінці *Бази документів* натиснути кнопку *Дозволити доступ*).

3) Запустити програму *Відновлення пошкодженої бази документів* (%LOZA%\LIB\RecoverDamagedBase.exe).

4) Вибрати папку, що містить пошкоджену базу документів.

Всі бази зберігаються в кореневій директорії відповідного диска у папці LOZADoc. Ця папка є прихованою (має атрибут Hidden, Скрытый), тому для того, щоб вона відображалась у діалозі вибору папки, необхідно відповідним чином настроїти параметри відображення папок.

Вибрати можна кореневу папку, що містить усі бази документів на диску (наприклад, C:\LOZADoc) або папку, що містить конкретну пошкоджену базу (наприклад, C:\LozaDoc\0). В останньому випадку буде проаналізована тільки обрану базу.

5) За допомогою кнопки *Відновити базу документів* виконати відновлення. Під час відновлення проводиться аналіз коректності службових файлів та виконуються такі дії:

– якщо пошкоджено головний службовий файл бази документів (її опис), за можливості він відновлюється; атрибути бази встановлюються таким чином:

  – назва бази: *Відновлена база №…*;
  – керування доступом: *Адміністративне*;
  – власник бази: значення обирається вручну із запропонованого списку;
  – максимальний та мінімальний рівень доступу: визначаються за списком документів, якщо це можливо, інакше встановлюються значення *Таємно* та *Відкрита інформація*;
  – дозволи на доступ до бази, аудит доступу до бази, дозволи на доступ до документів та аудит доступу до документів встановлюються так, як при створенні нової бази;
  – службова інформація береться із наявного списку документів;

– якщо пошкоджений файл зі списком документів у будь-якій папці бази документів, він відновлюється із списку файлів та опису бази; атрибути документів встановлюються таким чином:

– назва документу: використовується код документу;

– дати створення та модифікації встановлюється за датами створення та модифікації файлу, що відповідає документу;

– рівень доступу: максимальний рівень доступу для бази документів;

– власник документа: власник бази документів;

– списки доступу та аудиту визначаються списками доступу та аудиту документів для відповідної бази документів;

– інформація про оформлення не відновлюється;

– якщо пошкоджений довідник типів документів, то створюється новий порожній довідник.

Інформація про результат відновлення видається у вигляді, представленому на рисунку 5.2.

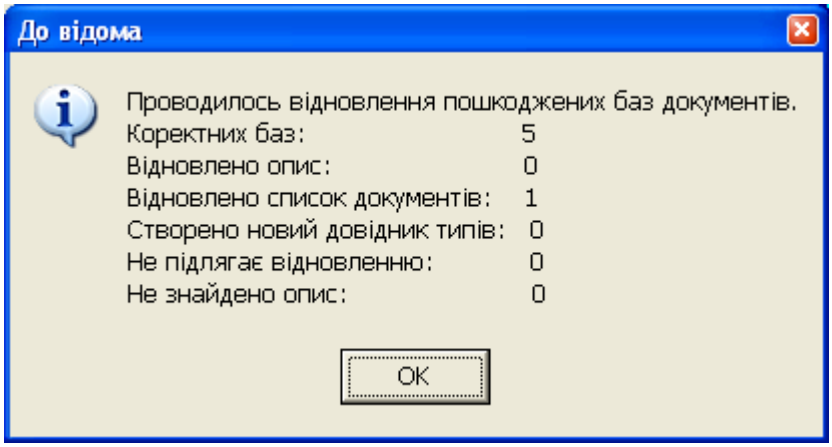

Рисунок 5.2 – Звіт про відновлення

6) Якщо відновлена база зберігається на жорсткому диску, треба за допомогою програми *Помічник адміністратора* (%LOZA%\LIB\AdminAssistant.exe) заборонити доступ до баз документів (на сторінці *Бази документів* натиснути кнопку *Заборонити доступ*).

7) Адміністратор документів та, можливо, інші користувачі (наприклад, власники документів) повинні відновити втрачену інформацію про бази та документи, зокрема, списки доступу та аудита, якщо вони повинні відрізнятись від тих, що встановлюються за умовчанням, а також назви документів.

Перелік скорочень

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

Параметри конфігурації системи виділено `рівномірним шрифтом`.