Товариство з обмеженою відповідальністю
Науково-дослідний інститут
«Автопром»

Система захисту інформації

ЛОЗА™-2

версія 2

редакція 2.5.4

ІНСТРУКЦІЯ КОРИСТУВАЧА

ЛОЗА-2.І3.02.1

ТОВ НДІ “Автопром”
Київ, 2009

Зміст

1 Загальні положення

Документ призначений для користувачів, які працюють із системою захисту інформації ЛОЗА-2. Він містить загальні правила роботи в системі, необхідні всім користувачам, незалежно від ролі, яку вони виконують.

Користувачі системи ЛОЗА-2 повинні мати базові навички роботи з обчислювальною технікою, з операційною системою Windows 2000/XP/2003 та із програмами MS Word та MS Excel із набору MS Office 97/2000/XP/2003/2007.

2 Порядок роботи в системі

Після встановлення системи ЛОЗА-2 під час входу користувача до Windows, розблокування комп'ютера, завершення роботи тощо використовуватимуться аналогічні діалоги системи ЛОЗА-2 (вони зображені на наведених нижче рисунках).

2.1 Ім'я, пароль та ключовий диск користувача

Для роботи в системі кожний користувач отримує від адміністратора безпеки ім'я та пароль. За необхідності користувач отримує також ключовий диск, необхідний для автентифікації, який поряд із паролем використовуватиметься для підтвердження особистості користувача.

2.1.1 Ім'я користувача

Ім'я користувача не залежить від регістра і визначається адміністратором безпеки за правилами, прийнятими у Windows:

– може містити до 20 символів за винятком таких:

" / \ [ ] : ; | = , + * ? < >

– не може містити лиш крапки та пропуски.

2.1.2 Пароль користувача

Пароль для першого входу в систему визначається адміністратором безпеки. Під час першого входу система пропонує користувачеві змінити пароль. Таким чином, пароль користувача знатиме тільки він сам. Користувач повинен своєчасно (орієнтовно – раз на місяць) змінювати пароль. Для зміни пароля необхідно натиснути клавіші *Ctrl+Alt+Delete* та кнопку *Смена пароля* (*Зміна пароля*). Вікно, призначене для зміни пароля, наведене на рис 2.1.

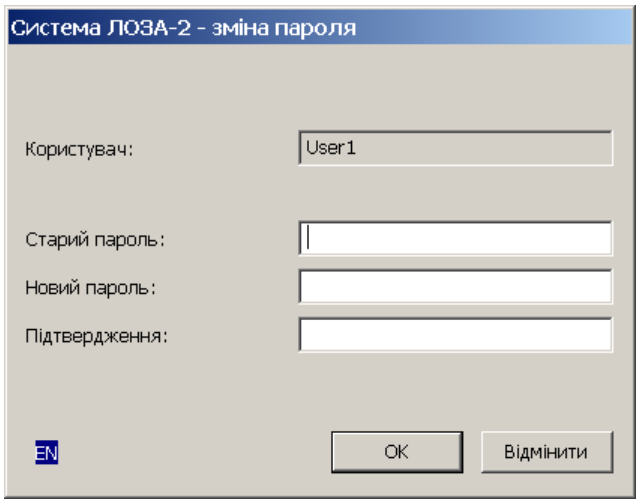

Рисунок 2.1

Якщо встановлені відповідні настройки, система вимагатиме від користувача, щоб пароль задовольняв таким обмеженням:

а) містив не менше 6 символів;

б) містив символи хоча б із трьох наборів із наведених чотирьох:

– прописні літери латинського, російського та українського алфавітів: A,B,C,D,…,Z, А, Б,…Я;

– строкові літери латинського, російського та українського алфавітів: a,b,c,d,…,z, а, б,…я;

– цифри: 0,1,2,3,…,9;

– спеціальні символи:

~ ` ! @ # $ % ^ & * ( ) _ - + = | \ { } [ ] : ; ” ’ < > , . ?

в) не містив у собі ім’я користувача чи частину його повного імені;

г) відрізнявся від двох попередніх паролів користувача

Коли наближається термін зміни пароля, при реєстрації користувач отримує повідомлення про це. Якщо пароль не буде змінений вчасно, система змусить користувача зробити це під час чергового входу до системи.

2.1.3 Ключовий диск користувача

Як ключові диски можуть використовуватись дискети та модулі пам’яті USB Flash.

Кожний користувач може мати два ключові диски – основний та резервний, які надають йому однакові повноваження.

Перед тим як видати користувачеві його ключовий диск, адміністратор безпеки повинен ініціалізувати його.

Кожний користувач системи може мати два ключових диски – основний та резервний, які надають йому однакові повноваження. Використання одного й того ж ключового диска для різних користувачів комп’ютері неможливо. Неможливо також використання одного й того ж диска як основного і резервного.

Адміністратор безпеки встановлює, коли саме система перевіряє наявність ключового диска. Ця перевірка може виконуватись:

– під час входу користувача до Windows;

– під час роботи користувача із засобами системи ЛОЗА-2;

– під час роботи користувача у Windows.

Якщо встановлена перевірка ключових дисків під час роботи у Windows, ключовий диск має бути встановлений постійно під час роботи користувача за комп’ютером. Одразу після видалення ключового диска комп’ютер автоматично блокується, а для того, щоб його розблокувати, необхідно встановити ключовий диск (п. 2.5).

2.2 Комп’ютери, за якими може працювати користувач

Із своїм іменем, паролем та (в разі необхідності) ключовим диском користувач може працювати за будь-яким комп’ютером мережі, якщо це дозволено адміністратором. Адміністратор безпеки може для кожного комп’ютера визначити перелік ролей користувачів, яким дозволено за ними працювати. Для сервера це звичайно *Адміністратор безпеки* та *Системний адміністратор*, для робочих станцій – повний перелік ролей (*Адміністратор безпеки*, *Системний адміністратор*, *Адміністратор документів* та *Звичайний користувач*).

2.3 Початок роботи

Для початку роботи в системі необхідно після відповідного запрошення натиснути клавіші *Ctrl-Alt-Delete* (рис. 2.2).

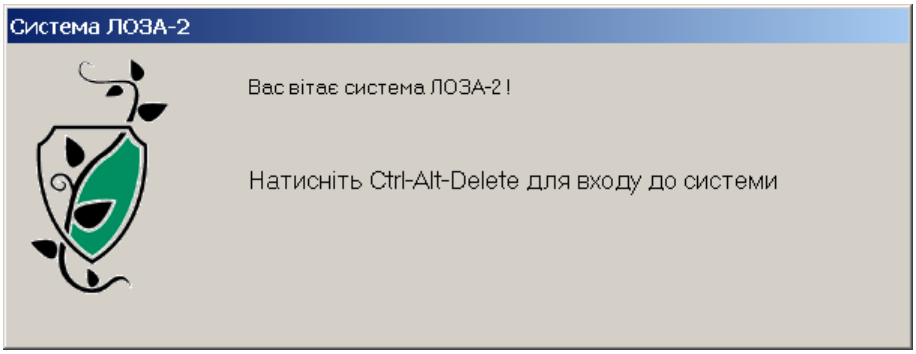

Рисунок 2.2

Далі необхідно зареєструватись в системі, тобто ввести своє ім’я і пароль та , за необхідності, встановити ключовий диск (рис. 2.3).

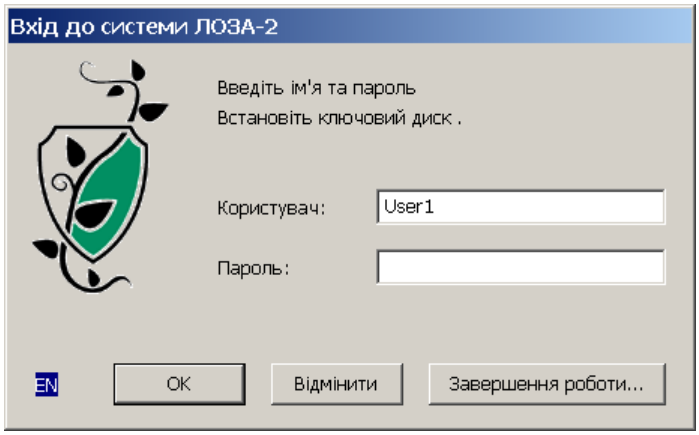

Рисунок 2.3

У випадку, коли ім’я або пароль декілька раз вводяться невірно (кількість спроб задається адміністратором безпеки), обліковий запис користувача блокується. Враховуються також невдалі спроби введення пароля під час розблокування комп’ютера та зміни пароля. Розблокувати обліковий запис може тільки адміністратор безпеки.

2.4 Повідомлення під час роботи

Під час роботи в системі користувач може отримати повідомлення про аварійне завершення роботи. У такому випадку користувач має закінчити сеанс роботи або вимкнути комп’ютер.

2.5 Захист інформації у період відсутності користувача

Після входу користувача до системи всі дії на комп’ютері виконуються від його імені, тому до виходу із системи комп’ютер не можна залишати без нагляду. Виконання цієї вимоги не дає можливості іншим користувачам отримати доступ до інформації від імені користувача, що зареєструвався.

У разі необхідності залишити комп’ютер на короткий час необхідно заблокувати комп’ютер. Для цього в тому разі, коли встановлена перевірка ключових дисків під час роботи у Windows (п. 2.1.3), достатньо вийняти ключовий диск, у протилежному випадку – натиснути клавіші *Ctrl-Alt-Delete* і у вікні, що з’явиться на екрані (рис. 2.4), – кнопку *Блокування*.

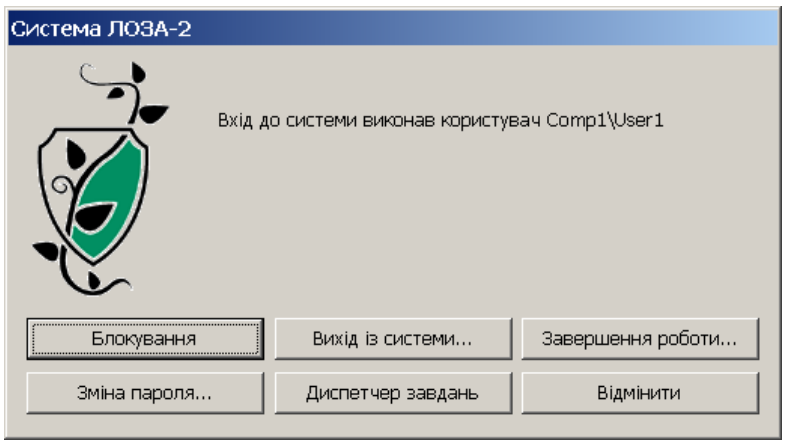

Рисунок 2.4

Після цього доступ до комп'ютера буде заблокований (рис. 2.5), і робота на ньому стане неможливою до зняття блокування.

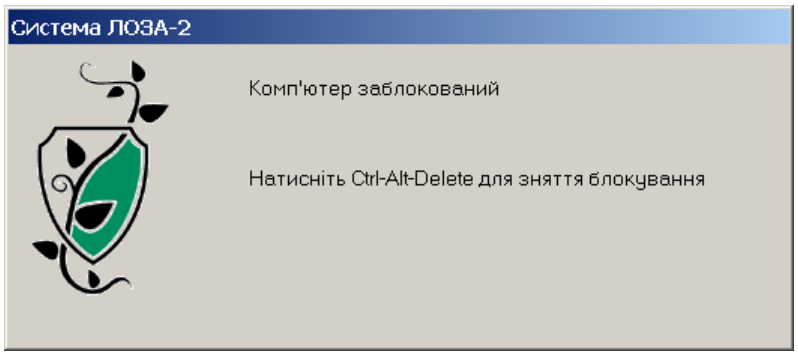

Рисунок 2.5

Для того щоб зняти блокування (рис. 2.6) необхідно:

– натиснути клавіші *Ctrl-Alt-Delete*;
– ввести своє ім'я і пароль та, за необхідності, встановити ключовий диск.

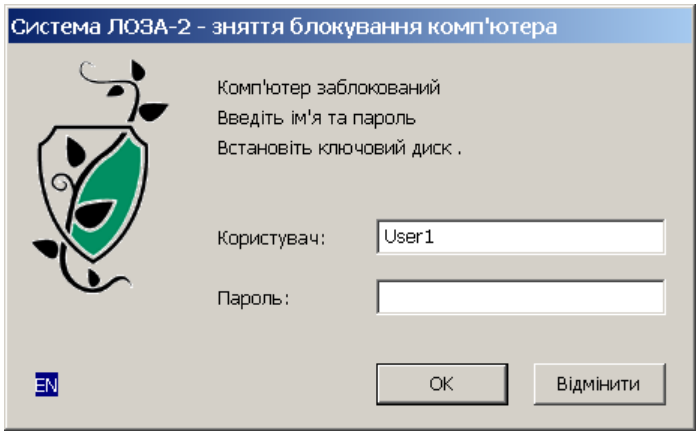

Рисунок 2.6

Якщо користувач, який заблокував комп'ютер, з якоїсь причини не може його розблокувати, це може зробити адміністратор безпеки. У такому випадку всі дані, які користувач не зберіг перед блокуванням, будуть втрачені.

2.6 Закінчення роботи

Для закінчення роботи необхідно закінчити роботу всіх програм і натиснути клавіші *Ctrl-Alt-Delete*. Після цього на екрані з'являється вікно (рис. 2.7), у якому необхідно обрати спосіб завершення роботи.

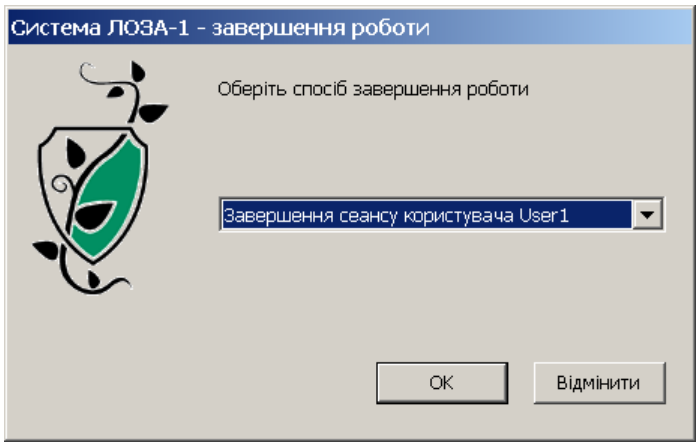

Рисунок 2.7

Робота може бути завершена одним із таких трьох способів:

- завершення сеансу;
- завершення роботи;
- перезавантаження.