

Товариство з обмеженою відповідальністю  
**Науково-дослідний інститут  
«Автопром»**

**Система захисту інформації**

**ЛОЗА™-1**

**версія 2**

**редакція 2.5.11**

---

**ІНСТРУКЦІЯ  
АДМІНІСТРАТОРА БЕЗПЕКИ**

ЛОЗА-1.ІЗ.01.2



ТОВ НДІ «Автопром»  
Київ, 2011

# Зміст

Вступ .....	3
<b>1 Ведення бази даних захисту .....</b>	<b>3</b>
1.1 Облікові записи користувачів .....	3
1.2 Ключові диски .....	4
1.3 Ототожнення .....	4
1.4 Архівування та відновлення бази даних захисту .....	5
<b>2 Налаштування системи .....</b>	<b>5</b>
2.1 Встановлення дозволів на доступ до даних захисту .....	5
2.2 Встановлення параметрів входу до системи .....	6
2.3 Встановлення параметрів захисту друку та експорту документів .....	7
2.4 Встановлення параметрів ключових дисків .....	7
2.5 Встановлення параметрів роботи зі знімними дисками .....	8
2.5.1 Диски для зберігання документів .....	8
2.5.2 Блокування дисків .....	8
2.6 Встановлення параметрів заборони друку .....	9
2.7 Встановлення політики аудита .....	10
2.8 Встановлення політики блокування облікового запису .....	10
2.9 Встановлення політики документів .....	11
2.10 Встановлення політики паролів .....	12
<b>3 Спостереження за роботою системи .....</b>	<b>13</b>
<b>4 Зміна власника баз та документів .....</b>	<b>13</b>
<b>5 Відновлення доступу до баз та документів .....</b>	<b>13</b>
<b>6 Перелік скорочень та позначень .....</b>	<b>15</b>

## Вступ

Документ “Інструкція адміністратора безпеки” є складовою частиною експлуатаційної документації на систему захисту інформації ЛОЗА-1. Він призначений для працівника (працівників), якому встановлено роль *Адміністратор безпеки*.

Адміністратор безпеки виконує в системі такі функції:

- ведення бази даних захисту;
- настройка системи – встановлення значень параметрів конфігурації системи, безпосередньо пов’язаних із доступом до інформації;
- спостереження за роботою системи;
- зміна у разі необхідності власника баз документів та документів.

З огляду на особливості автоматизованої системи, у якій буде використовуватись система ЛОЗА-1, документ може бути доповнений.

Адміністратор безпеки повинен мати базові навички роботи з операційною системою Microsoft Windows 2000/XP, а також розуміти основи функціонування системи ЛОЗА-1, які викладено в документі “Загальний опис системи” (відомості із цього документа використовуються далі без посилання на нього).

Для виконання більшості своїх завдань адміністратор безпеки використовує програми *Аудитор*, *Керування захистом* та *Монітор захисту*. Ці програмні засоби докладно описано в документі “Програмні засоби адміністрування системи. Інструкція користувача”.

## 1 Ведення бази даних захисту

### 1.1 Облікові записи користувачів

База даних захисту містить перелік користувачів системи з їхніми атрибутами доступу. Для ведення бази даних захисту використовується програма *Керування захистом*.

Кожний користувач системи ЛОЗА-1 повинен мати обліковий запис у Windows. Під час створення облікового запису в системі ЛОЗА-1 адміністратор безпеки може вибрати один із облікових записів Windows (для яких ще не створені облікові записи в системі ЛОЗА-1) або створити новий обліковий запис.

Якщо адміністратор створює новий обліковий запис, відповідний обліковий запис буде створений у Windows. Після встановлення властивостей облікового запису системи ЛОЗА-1 встановлюються відповідні властивості облікового запису Windows. Новому користувачеві необхідно надати умовний пароль і встановити відмітку, яка вимагає змінити пароль при наступному вході до системи. Таким чином, при першому вході до системи користувач буде змушений змінити пароль, у результаті знатиме його тільки він сам.

Якщо хоча б один з параметрів конфігурації

- перевіряти ключовий диск під час входу до Windows;
- перевіряти ключовий диск під час роботи у Windows,

має значення *Так*, після введення нового користувача йому необхідно ініціалізувати один або два ключові диски.

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

## 1.2 Ключові диски

У випадку, коли один з параметрів, наведених в п. 1.1, має значення *Так*, робота користувача за комп'ютером можлива тільки за наявності ключового диска. Ключовий диск користувача створює адміністратор.

На одному комп'ютері кожний користувач може мати два ключових диски – основний та резервний, які надають йому однакові повноваження. Один і той же ключовий диск може використовуватись на різних комп'ютерах. Для того щоб скористатись цією можливістю, треба виконати такі дії:

- під час створення ключового диска на першому комп'ютері обрати опцію *ініціалізувати новий ключовий диск*;
- під час створення ключового диска на інших комп'ютерах обрати опцію *запам'ятати існуючий ключовий диск*.

Використання одного й того ж ключового диска для різних користувачів на одному комп'ютері неможливо. Неможливо також використання одного й того ж диска як основного і резервного.

## 1.3 Ототожнення

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 один користувач працює на комп'ютерах *K1* та *K2* під іменем *User1*, а інший користувач працює на тих же комп'ютерах під іменем *User2*. Нижче описаний процес встановлення ототожнень.

1) На комп'ютері *K1* за допомогою програми *Керування доступом* відкрити перелік користувачів та виконати його експорт на знімний носій. Припустимо, що адміністратор безпеки назвав файл із експортованим списком *K1\_Users.cds*.

2) На комп'ютері *K2* за допомогою програми *Керування доступом* відкрити перелік користувачів.

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

- обрати пункт меню *Ототожнення*;
- у діалозі вказати файл *K1\_Users.cds*;
- обрати в переліку рядок *K1\User1*;
- зберегти ототожнення.

4) Таким же чином встановити ототожнення для користувача *User2*.

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

## 1.4 Архівування та відновлення бази даних захисту

Адміністратор безпеки повинен періодично виконувати архівування бази даних захисту. Орієнтовна періодичність архівування – один раз на місяць, але, якщо після останнього архівування зміни до переліку користувачів не вносились, чергове архівування не потрібне.

База даних захисту складається з одного файлу – переліку користувачів, саме його і треба архівувати. Для цього за допомогою програми *Керування захистом* перелік користувачів необхідно експортувати. Файл, який буде отримано в результаті експорту, є копією бази даних захисту.

У випадку необхідності база даних захисту може бути відновлена з резервної копії. Для цього за допомогою програми *Керування захистом* слід імпортувати резервну копію переліку користувачів. Це особливо корисно після переінсталяції операційної системи. Під час імпорту в системі будуть створені всі користувачі, які існували в попередній інсталяції, а також будуть відновлені всі їхні атрибути, у тому числі ролі, рівні доступу, паролі та ключові диски.

## 2 Налаштування системи

Для встановлення значень параметрів конфігурації системи використовується програма *Керування захистом*.

Адміністратор безпеки має можливість встановлювати значення всіх параметрів конфігурації системи. Для більшості параметрів такі ж повноваження має системний адміністратор.

Правила розмежування доступу виділяють декілька груп параметрів, доступ до яких має тільки адміністратор безпеки. Це групи параметрів, безпосередньо пов'язані з керуванням доступом:

- дозволи на доступ до даних захисту;
- параметри входу до системи;
- параметри захисту друку та експорту документів;
- параметри ключових дисків;
- диски для зберігання документів;
- параметри блокування дисків;
- параметри заборони друку;
- політика аудита;
- політика блокування облікового запису;
- політика документів;
- політика паролів.

Перелік усіх параметрів конфігурації наведено в Додатку А документа „Загальний опис системи”.

Нижче наведені докладні пояснення щодо встановлення значень цих параметрів конфігурації.

### 2.1 Встановлення дозволів на доступ до даних захисту

Дозволи на доступ до даних захисту визначаються параметром конфігурації системи дозволи на доступ до даних захисту. За допомогою цього параметра для користувачів із ролями *Адміністратор безпеки* та *Системний адміністратор* встановлюються дозволи на читання та запис для кожної зі складових даних захисту:

- бази даних захисту (перелік користувачів з їхніми атрибутами доступу та даними, необхідними для автентифікації);
- параметрів конфігурації системи;
- оперативних даних про роботу системи;
- журналу захисту.

Для параметрів конфігурації дозволи надаються для груп параметрів.

Дозволи на доступ до складових даних захисту, які безпосередньо пов'язані з керуванням доступом, зафіксовані і не можуть бути змінені. Для цих складових дозвіл на читання та запис має лише адміністратор безпеки. Системний адміністратор доступу до них не має. Інші дозволи встановлюються на розсуд адміністратора безпеки.

Змінювати значення за умовчанням для параметра дозволи на доступ до даних захисту необхідно лише в особливих випадках.

## 2.2 Встановлення параметрів входу до системи

Вхід до системи регулюється такими параметрами конфігурації системи:

- дозволяти вхід до Windows тільки користувачам системи;
- перевіряти ключовий диск під час входу до Windows;
- перевіряти ключовий диск під час роботи у Windows;
- відображати ім'я попереднього користувача;
- дозволяти вхід до Windows тільки в робочому стані системи.

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

Якщо параметр конфігурації *Дозволяти вхід до Windows тільки користувачам системи* має значення *Так*, це матиме такі наслідки:

- увійти до Windows зможуть тільки користувачі, які мають обліковий запис у системі ЛОЗА-1;
- замість стандартних діалогів входу до Windows, виходу з Windows (викликається натисканням комбінації клавіш Ctrl+Alt+Del після успішного входу до системи), розблокування комп'ютера та зміни пароля використовуватимуться відповідні діалоги системи ЛОЗА-1;
- під час входу до системи користувачі будуть змушені використовувати комбінацію клавіш Ctrl+Alt+Del;
- буде відключена можливість запуску програм від імені іншого користувача;
- будуть відключені екран привітання Windows XP та можливість швидкого переключення між користувачами Windows XP.

Значення параметрів відображати ім'я попереднього користувача, дозволяти вхід до Windows тільки в робочому стані системи та перевіряти ключовий диск під час входу до Windows можна встановлювати тільки в тому випадку, коли для параметра дозволяти вхід до Windows тільки користувачам системи встановлене значення *Так*.

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.

Значення *Так* параметра конфігурації *перевіряти ключовий диск під час роботи у Windows* означає, що у випадку видалення ключового диска під час роботи комп'ютер автоматично блокується. Значення цього параметра можна

встановлювати тільки в тому випадку, коли для параметра перевіряти ключовий диск під час входу до Windows встановлене значення *Так*.

Значення *Так* параметра конфігурації *відображати ім'я попереднього користувача* означає, що в діалозі входу до системи буде відображатись ім'я попереднього користувача.

Значення *Так* параметра конфігурації *дозволяти вхід до Windows тільки в робочому стані системи* означає, що звичайні користувачі та адміністратори документів можуть увійти до Windows тільки під час перебування системи в робочому стані.

### **2.3 Встановлення параметрів захисту друку та експорту документів**

Система надає можливості для захисту документів під час їх друку та експорту (збереження у файлі). Ці можливості рекомендується використовувати при роботі із секретною інформацією.

Захист друку документів регулюється за допомогою таких параметрів конфігурації:

- захищати друк документів паролем;
- пароль на друк документів.

Надання параметру конфігурації захищати друк документів паролем значення *Так* означає, що користувач отримуватиме доступ на друк документа лише за умови введення паролю на друк, що забезпечує присутність під час друку уповноваженої особи.

Для встановлення пароля адміністратор за допомогою програми *Керування захистом* викликає відповідне вікно та запрошує уповноважену особу ввести пароль.

Обмеження для пароля (мінімальна довжина, складність, термін дії і т. ін.) не передбачаються, – уповноважена особа, що використовує пароль, встановлює відповідні правила на власний розсуд.

Захист експорту документів здійснюється аналогічним чином. Для цього використовуються такі параметри конфігурації:

- захищати експорт документів паролем;
- пароль на експорт документів.

### **2.4 Встановлення параметрів ключових дисків**

Системі надає можливість використовувати для автентифікації користувача не тільки пароль, а й фізичні ідентифікатори – ключові диски, що значно підвищує надійність автентифікації.

Як ключові диски можуть використовуватись дискети та/або модулі пам'яті USB Flash із файловою системою FAT.

Використання ключових дисків регулюється такими параметрами конфігурації системи:

- гнучкі ключові диски;
- знімні ключові диски.

Ці параметри встановлюють, які саме диски будуть використовуватись для автентифікації користувача. Для автентифікації можуть використовуватись всі гнучкі та/або знімні диски або вибрані.

## 2.5 Встановлення параметрів роботи зі знімними дисками

### 2.5.1 Диски для зберігання документів

Система ЛОЗА-1 дозволяє зберігати бази документів на жорсткому диску та на знімних носіях – дискетах, модулях пам'яті USB Flash, компакт-дисках (без можливості запису), Zip-дисках тощо.

Для того щоб адміністратор безпеки мав змогу вказати, де саме повинні зберігатись бази документів, використовуються такі параметри конфігурації:

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

Всі параметри можуть приймати значення *Всі диски* або містити фіксований перелік букв, які відповідають дискам певного типу (наприклад, *F*, *G*:).

Документи зберігаються в кореневій папці зазначеного диска в папці LOZADoc.

Зберігати документи на жорстких дисках (тобто на розділах жорсткого диска) можна лише в тому випадку, коли вони використовують файлову систему NTFS. Для в папки LOZADoc на фіксованому диску встановлюються ті ж дозволи на доступ, що і для папки %LOZA%\Doc. Це унеможливує доступ до папки для всіх користувачів системи. Незмінність встановлених дозволів перевіряється під час перевірки цілісності файлів та папок.

Для унеможливлення доступу користувачів до документів, які зберігаються на гнучких дисках, компакт-дисках та знімних дисках, рекомендується блокувати ці диски (див. п. 2.5.2).

### 2.5.2 Блокування дисків

Блокування дисків використовується для унеможливлення безпосереднього доступу звичайних користувачів до даних, які зберігаються на знімних носіях.

Звичайні користувачі та адміністратори документів безпосереднього доступу до заблокованого диска не мають. Вони можуть отримати доступ до даних лише за допомогою програми *Захищені документи*. Адміністратори безпеки та системні адміністратори мають до заблокованого диска повний доступ.

Заблокувати можна будь-яку кількість знімних дисків. Диски блокуються на весь час роботи системи, незалежно від стану, у якому вона перебуває. Перелік знімних дисків, які блокуються, визначається такими параметрами конфігурації:

- блокування гнучких дисків;
- блокування знімних дисків;
- блокування компакт-дисків.

Параметри блокувати знімні диски та блокувати компакт-диски можуть приймати лише два значення: *всі диски* та *всі диски з документами*. Значення *всі диски з документами* означає, що блокуватись будуть лише ті диски, на яких зберігаються бази документів.

Для параметра блокувати гнучкі диски можуть бути вказані значення *не блокувати* та *всі диски* або явно вказані диски, які слід блокувати (наприклад, диск A:).

Ці параметри дозволяють виконати одночасно два описані нижче завдання.

1) Заблокувати всі диски, на яких зберігаються бази документів. Блокування цих дисків є необхідною умовою використання системи ЛОЗА-1.



Знімні диски та компакт-диски, на яких зберігаються бази документів, будуть заблоковані автоматично, а для гнучких дисків блокування повинен встановити адміністратор.

2) Заблокувати взагалі всі знімні диски або всі знімні диски певного типу на комп'ютері. Це може бути необхідно, наприклад, для унеможливлення неконтрольованого використання знімних дисків.

## **2.6 Встановлення параметрів заборони друку**

Система ЛОЗА-1 надає можливість повністю контролювати друк документів, які обробляються за допомогою програми *Захищені документи*. Для цього можуть бути використані такі механізми:

- встановлення дозволу/заборони друку документа;
- встановлення аудиту друку документа, що забезпечує докладну реєстрацію подій друку;
- встановлення пароля на друк.

Під час роботи за допомогою інших програмних засобів перелічені механізми не можуть бути задіяні. Для таких випадків у системі передбачена можливість повної або часткової заборони друку, а також можливість тимчасового дозволу друку.

Для встановлення заборони друку використовуються два параметри конфігурації:

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

Перший параметр визначає, кому саме заборонений друк, і може приймати такі значення:

- нікому (друк дозволений всім);
- всім (друк заборонений всім);
- всім користувачам системи ЛОЗА-1, крім адміністраторів безпеки;
- всім користувачам системи ЛОЗА-1, крім адміністраторів документів;
- всім користувачам системи ЛОЗА-1, крім адміністраторів безпеки та документів;
- спеціальна настройка.

Якщо параметр спосіб заборони друку має значення спеціальна настройка, друк забороняється для облікових записів, які перелічені в параметрі облікові записи для заборони друку.

Заборона друку, яка визначається зазначеними параметрами, встановлюється на початку роботи системи та під час кожного входу користувача до системи (якщо для параметра дозволяти вхід до Windows тільки користувачам системи має значення *Так*).

Для того, щоб тимчасово дозволити користувачу друк, не вимагаючи його виходу із системи, адміністратор може скористатись утилітою *Помічник адміністратора*, яка заходить у папку %LOZA%\Lib (файл AdminAssistant.exe).

Після запуску утиліти адміністратор повинен вказати своє ім'я, пароль та ключовий диск (останнє – якщо параметра перевіряти ключовий диск під час входу до Windows має значення *Так*). Утиліта надає можливість тимчасово дозволити друк. Адміністратор вказує також «термін дії» тимчасового дозволу на друк, обираючи один з двох варіантів:

- *до заборони друку адміністратором* – це означає, що для відновлення заборони друку адміністратор повинен знову скористатись утилітою *Помічник адміністратора*;
- *поки встановлений ключовий диск адміністратора* (цей варіант доступний лише тоді, коли параметр перевіряти ключовий диск під час входу до Windows має значення *Так*).

## **2.7 Встановлення політики аудита**

Політика аудита визначається однойменним параметром конфігурації системи (параметр політика аудита) визначає, які саме дії користувачів можуть бути зареєстровані в журналі захисту. Політика аудита встановлюється окремо для таких категорій:

- *вхід/вихід* (вхід користувачів до системи ЛОЗА-1, зміна пароля користувача, вихід із системи та ін.);
- *робота з програмами* (запуск та завершення роботи прикладних програм системи);
- *керування доступом* (коригування бази даних захисту);
- *керування системою* (зміна стану системи, визначення початкового стану для наступного сеансу роботи та ін.);
- *конфігурація* (читання та зміна значень параметрів конфігурації);
- *доступ до документів* (читання, коригування, друк документів, коригування атрибутів доступу документів та ін.);
- *доступ до баз документів*.

Встановлення аудита для всіх категорій, крім двох останніх, призводить безпосередньо до реєстрації відповідних подій у журналі.

Встановлення аудита подій доступу до документів та баз документів лише дозволяє реєстрацію відповідних подій. Для того щоб вони були зареєстровані, необхідно щоб аудит був також встановлений у списку аудита відповідного об'єкта.

Політика аудита може бути встановлена досить гранульовано. Для параметрів конфігурації аудит може бути встановлений окремо для різних груп параметрів. Для подій доступу до документів аудит може бути встановлений у залежності від рівня доступу документа, а для подій доступу до баз документів – у залежності від максимального рівня доступу бази.

Значення за умовчанням політики аудита обрано таким чином, щоб у журналі реєструвались всі події, важливі з точки зору захисту інформації, а, з іншого боку, на реєструвались малозмістовні події, які лише захаращують журнал. Змінювати це значення рекомендується тільки в особливих випадках (наприклад, у разі виникнення обставин, які вказують на можливий витік секретної інформації).

## **2.8 Встановлення політики блокування облікового запису**

Політика блокування облікового запису використовується для підвищення стійкості до підбору паролів. Вона визначається такими параметрами конфігурації системи:

- інтервал для поновлення відліку невдалих спроб входу до системи;
- максимальна кількість невдалих спроб входу до системи.

Параметр максимальна кількість невдалих спроб входу до системи вказує кількість невдалих спроб входу до системи, після яких обліковий запис блокується. Як невдалі спроби входу зраховуються всі спроби входу, спроби

розблокування комп'ютера та спроби зміни пароля, під час яких користувач вказує невірний пароль.

Параметр інтервал для поновлення відліку невдалих спроб входу до системи визначає інтервал, після закінчення якого відлік невдалих спроб входу поновлюється.

Політика блокування облікового запису застосовується тільки в тому випадку, коли для параметра дозволяти вхід до Windows тільки користувачам системи задане значення *Так*.

## 2.9 Встановлення політики документів

Політика документів встановлює декілька загальних обмежень на роботу з документами. Вона визначається такими параметрами 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 та експортом.

Параметр конфігурації максимальний рівень доступу документів визначає максимальний рівень доступу документів, які можуть міститись в базах документів.

Якщо параметр конфігурації обмеження для адміністратора документів має значення *Так*, це 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.

Якщо параметр конфігурації *дозволяти створення довірчих баз* має значення *Так*, це означає, що в системі дозволяється створювати бази з довірчим керуванням доступом.

Значення параметра максимальний рівень доступу для довірчих баз визначає 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*.

Якщо параметр конфігурації реєстрація подій для довірчих баз має значення *Ні*, для баз із довірчим керуванням доступом аудит на здійснюється, незалежно від того, чи встановлений аудит у списках доступу баз та документів.

Параметр конфігурації примусове маркування документів перед друком та експортом може мати значення *Так* та *Ні*. Якщо він має значення *Так*, 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.

## 2.10 Встановлення політики паролів

Політика паролів використовується для підвищення стійкості до підбору паролів. Вона визначається такими параметрами конфігурації:

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

Параметр кількість неповторюваних паролів обмежує можливість користувачів використовувати старі паролі під час зміни пароля.

Параметр максимальний термін дії пароля визначає термін, після закінчення якого система змушує користувача змінити пароль.

Параметр мінімальна довжина пароля не дозволяє використовувати занадто короткі паролі.

Параметр паролі повинні задовольняти вимогам щодо складності змушує користувача використовувати досить складні паролі. Складність пароля означає виконання таких вимог:

- пароль не повинен містити в собі ім'я або повне ім'я користувача;
- пароль має містити символи хоча б із трьох наборів із наведених чотирьох:
  - прописні літери латинського, російського та українського алфавітів;
  - строкові літери латинського, російського та українського алфавітів;
  - цифри;
  - спеціальні символи:

~ ` ! @ # \$ % ^ & \* ( ) \_ - + = | \ { }

Політика паролів застосовується тільки в тому випадку, коли для параметра дозволяти вхід до Windows тільки користувачам системи задане значення *Так*.

### 3 Спостереження за роботою системи

Під час роботи система відстежує небезпечні події, тобто події, які можуть вплинути на безпеку інформації. У разі виникнення таких подій звіт із відповідними відомостями автоматично друкується та/або зберігається у файлі (згідно з параметром конфігурації створення звіту про небезпечні події). Цей файл створюється в папці %LOZA%\Security\Log\Report. Виникнення файлу звіту на диску слугує адміністратору сигналом про можливе порушення безпеки інформації.

Адміністратор має періодично переглядати вказану папку і аналізувати звіти, які в ній з'являються. Він має з'ясувати причину виникнення кожної з небезпечних подій і за необхідності вжити відповідних заходів.

Те, які саме події вважаються небезпечними, визначається двома параметрами конфігурації:

- перелік небезпечних подій;
- вважати помилки небезпечними подіями.

Рекомендований перелік небезпечних подій із докладними поясненнями наведений у Додатку В документа “Загальний опис системи”. Після накопичення досвіду аналізу звітів адміністратор може змінювати цей перелік.

У разі необхідності адміністратор безпеки може створити протокол друку, який містить інформацію про друк документів, що містять інформацію з обмеженим доступом, та протокол за вибором, для якого критерії відбору подій визначаються довільним чином. Для створення цих протоколів використовується програма *Аудитор*.

### 4 Зміна власника баз та документів

За відсутності (через хворобу, відпустку, звільнення тощо) власника документа або бази документів може виникнути ситуація, коли жодний із користувачів системи не матиме доступу до цього документа або бази. У такому випадку адміністратор повинен відповідним чином встановити нового власника. Зміна власника виконується для таких об'єктів:

- бази документів із довірчим керуванням доступом та документи, які в них зберігаються;
- бази документів з адміністративним керуванням доступом.

Для зміни власника використовується програма *Захищені документи*.

### 5 Відновлення доступу до баз та документів

У випадку переінсталяції операційної системи доступ до баз та документів буде втрачений. Замість власника баз та документів, а також замість всіх облікових записів користувачів у списках доступу та аудита буде зазначений *Невідомий обліковий запис*. Відновити доступ можна двома описаними нижче шляхами. Для відновлення використовується програма *Захищені документи*.

1) Адміністратор безпеки згідно з п. 4 встановлює нового власника бази, а потім власник встановлює дозволи на доступ та аудит для бази та документів.

2) Якщо перед переінсталяцією операційної системи адміністратор виконав архівування (див. п. 1.4) бази даних захисту, а після інсталяції за допомогою імпорту або вручну створив користувачів з тими самими іменами, рівнями доступу та ролями, що й в попередній інсталяції, для відновлення доступу до бази документів та документів, які в ній зберігаються достатньо виконати такі дії:

- відкрити базу документів;

- обрати пункт меню *База – Відновити доступ*;
- в діалозі вибору файлу обрати копію бази даних захисту з попередньої інсталяції.

## **6 Перелік скорочень та позначень**

Параметри конфігурації системи захисту виділено рівномірним шрифтом.