Товариство з обмеженою відповідальністю
Науково-дослідний інститут
«Автопром»

Система захисту інформації

ЛОЗА™-2

версія 2

редакція 2.5.4

ІНСТРУКЦІЯ АДМІНІСТРАТОРА БЕЗПЕКИ

ЛОЗА-2.І3.01.1

ТОВ НДІ “Автопром”
Київ, 2009

Зміст

Вступ

Документ «Інструкція адміністратора безпеки» є складовою частиною експлуатаційної документації на систему захисту інформації ЛОЗА-2. Він призначений для працівника (працівників), якому встановлено роль *Адміністратор безпеки.*

Адміністратор безпеки виконує в системі такі функції:

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

Адміністратор безпеки повинен мати базові навички роботи з операційною системою Microsoft Windows 2000/XP/2003, а також розуміти основи функціонування системи ЛОЗА-2, 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 Інсталяція та деінсталяція системи

Інсталяція виконується згідно з документом «Інструкція з інсталяції». Інсталяція є нескладною процедурою, яка не вимагає від адміністратора глибокого знання операційної системи. Під час інсталяції пропонується вказати значення для деяких параметрів конфігурації системи, які згодом можна буде змінити за допомогою програми *Керування захистом*.

Користувач, який виконав інсталяцію, автоматично стає адміністратором безпеки системи ЛОЗА-2.

У разі необхідності адміністратор безпеки виконує також деінсталяцію системи (на сервері та/або на всіх або деяких робочих станціях), а також перенесення серверної частини системи на інший комп'ютер.

Під час деінсталяції системи з комп'ютера після відповідного підтвердження адміністратора можуть бути видалені всі документи, які зберігались на жорстких дисках цього комп'ютера. Для видалення використовується процедура, яка унеможливлює відновлення даних.

2 Ведення бази даних захисту

2.1 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-2 повинен мати обліковий запис в операційній системі сервера. Під час створення облікового запису в системі ЛОЗА-2 адміністратор безпеки може вибрати один із існуючих облікових записів (для яких ще не створені облікові записи в системі ЛОЗА-2) або створити новий обліковий запис.

Якщо адміністратор створює новий обліковий запис, відповідний обліковий запис буде створений в операційній системі сервера. Після встановлення властивостей облікового запису системи ЛОЗА-2 встановлюються відповідні властивості облікового запису в операційній системі сервера. 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.

2.2 Ключові диски

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

У випадку, коли один з параметрів, наведених в п. 2.1, має значення *Так*, робота користувача за комп'ютером можлива тільки за наявності ключового диска. Ключовий диск користувача створює адміністратор безпеки.

Під час створення ключового диска можна ініціалізувати новий диск, або запам'ятати існуючий (який був ініціалізований раніше).

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.

Один і той же ключовий диск може одночасно використовуватись у різних системах ЛОЗА-2 (тобто у різних локальних мережах). Для того щоб скористатись цією можливістю, треба виконати такі дії:

– під час створення ключового диска в першій системі обрати опцію *ініціалізувати новий ключовий диск*;

– під час створення ключового диска в інших системах обрати опцію *запам'ятати існуючий ключовий диск*.

2.3 Ототожнення

У тому випадку, коли користувачу необхідно працювати з документами, які зберігаються на знімному носії, у різних системах ЛОЗА-2 (тобто у різних локальних мережах), можливе виникнення ситуації, коли дозволи на доступ до документа або бази документів, надані в одній системі, не матимуть сили в іншій (незалежно від того, чи використовує користувач у різних системах 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 в різних системах один і той же користувач матиме різні SID'и. Для того щоб запобігти такій ситуації і надати користувачам можливість працювати з документами в різних системах, використовується *ототожнення* користувачів. Порядок встановлення ототожнень для користувачів простіше всього пояснити за допомогою простого приклада.

Припустимо, що користувач працює в системах *S1* та *S2* під іменем *User1* (співпадіння імен користувача в різних системах не є обов'язковим). Нижче описаний процес встановлення ототожнень.

1) У системі *S1* за допомогою програми *Керування захистом* відкрити перелік користувачів та виконати його експорт на знімний носій. Припустимо, що адміністратор безпеки назвав файл із експортованим списком *S1_Users.cds*.

2) У системі *S2* за допомогою програми *Керування захистом* відкрити перелік користувачів.

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

– обрати пункт меню *Ототожнення*;

– у діалозі вказати файл *S1_Users.cds*;

– обрати в переліку рядок *S1\User1*;

– зберегти ототожнення.

4) Повторити кроки 1) – 3) для встановлення ототожнень «у зворотному напрямку» (тобто виконати експорт переліку користувачів у системі *S2* та встановити ототожнення у системі *S1*).

2.4 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.

3 Настройка системи

Для встановлення значень параметрів конфігурації сервера та робочих станцій 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.

3.1 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;
- переліку робочих станцій;
- 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.

Параметр `дозволи на доступ до даних захисту` є загальним параметром системи і діє одночасно для всіх комп'ютерів мережі.

Змінювати значення за умовчанням для цього параметра необхідно лише в особливих випадках.

3.2 Захищені папки

Інколи виникає необхідність працювати з інформацією з обмеженим доступом, яка міститься не тільки в текстових документах Microsoft Word та електронних таблицях Microsoft Excel, а й у файлах інших форматів, для роботи з якими використовуються інші програмні засоби (наприклад, файли креслень, які обробляються за допомогою програми AutoCAD). Система ЛОЗА-2 надає можливість (з використанням засобів Windows) захистити такі дані. Захист здійснюється на рівні папок Windows. Для того щоб вказати, які саме папки слід захищати, використовується параметр конфігурації `перелік захищених папок`.

Захищена папка повинна знаходитись на томі з файловою системою NTFS. Для кожної захищеної папки виконуються такі дії:

– відслідковується цілісність дескриптора безпеки цієї папки (дескриптор безпеки поєднує власника, список доступу та список аудита);

– одразу після появи нового файлу або папки в захищеній папці власником цього файлу або папки стає група *Администраторы* Windows (в результаті звичайні користувачі, які створюють папки або файли в захищеній папці, не зможуть керувати доступом до цих об'єктів).

Після того як папка додається до переліку захищених папок, до переліку подій, які імпортуються до журналу захисту, додається подія #560 джерела *Security* (подія доступу до об'єктів, яку реєструє Windows) з умовою імпорту, згідно з якою подія імпортується в тому випадку, коли її опис містить рядок з іменем папки. У результаті журнал захисту міститиме всі події доступу до файлів та папок, які містяться в захищеній папці.

До переліку захищених папок рекомендується тимчасові папки, які використовуються користувачами під час імпорту та експорту документів.

3.3 Встановлення параметрів входу до системи

Вхід до системи регулюється такими параметрами конфігурації 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`;

– `дозволяти вхід до Windows за відсутності зв'язку із сервером`.

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-2 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.

Якщо для параметра `дозволяти вхід до Windows тільки в робочому стані системи` встановлене значення ***Так***, звичайні користувачі та адміністратори документів зможуть увійти до Windows тільки під час перебування системи ЛОЗА-2 в робочому стані. У випадку входу з робочої станції це означає, що в робочому стані повинні перебувати як сервер, так і робоча станція.

Якщо параметр `дозволяти вхід до Windows за відсутності зв'язку із сервером` має значення ***Так***, користувачі зможуть працювати за робочими станціями у автономному режимі, який активізується за відсутності зв'язку із сервером. У цьому режимі запуск програмних засобів системи ЛОЗА-2 неможливий.

Усі зазначені параметри є загальними параметрами системи і діють одночасно для всіх комп'ютерів мережі.

3.4 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`.

Якщо параметр `захищати друк документів паролем` має значення ***Так***, користувачі отримуватимуть 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`.

Усі зазначені параметри визначаються окремо для сервера і для кожної робочої станції (встановити одні й ті ж самі значення одночасно для в всіх комп'ютерів можна допомогою шаблона робочої станції).

3.5 Встановлення параметрів ключових дисків

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 диски для автентифікації;`
- `знімні диски для автентифікації.`

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

Зазначені параметри визначаються окремо для сервера і для кожної робочої станції (встановити одні й ті ж самі значення одночасно для в всіх комп'ютерів можна допомогою шаблона робочої станції).

3.6 Встановлення параметрів роботи зі знімними дисками

3.6.1 Диски для зберігання документів

Система ЛОЗА-2 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.`

Ці параметри встановлюються для кожного комп'ютера мережі. Диски сервера для зберігання документів можуть бути надані у спільне користування за допомогою таких параметрів:

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

Працювати із документами, які зберігаються на спільних дисках, можна з будь-якого комп'ютера мережі.

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

Документи зберігаються в кореневій папці зазначеного диска в папці LOZADoc.

Зберігати документи на фіксованих дисках (звичайно це розділи жорсткого диска) можна лише в тому випадку, коли вони використовують файлову систему NTFS. Для папки LOZADoc на фіксованому диску встановлюються дозволи на доступ, які унеможливлюють доступ до неї для всіх користувачів системи. Цілісність 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. 3.6.2).

3.6.2 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-2.

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.

3.7 Встановлення параметрів заборони друку

Система ЛОЗА-2 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-2, крім адміністраторів безпеки;

– всім користувачам системи ЛОЗА-2, крім адміністраторів документів;

– всім користувачам системи ЛОЗА-2, 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 папці %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*).

3.8 Встановлення політики аудита

Політика аудита визначається однойменним параметром конфігурації системи (параметр політика аудита). Вона 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-2, 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);

– *перелік робочих станцій* (читання та коригування переліку робочих станцій);

– *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 (документа чи бази документів).

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).

Політика аудита встановлюється окремо для сервера і для кожної робочої станції (встановити одне й те ж саме значення одночасно для в всіх комп'ютерів можна допомогою шаблона робочої станції).

3.9 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 зараховуються 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.

Параметри політики блокування облікового запису є загальними параметрами системи і діють одночасно для всіх комп'ютерів мережі.

3.10 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.

Параметри політики документів є загальними параметрами системи і діють одночасно для всіх комп'ютерів мережі.

3.11 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:

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

4 Ведення переліку робочих станцій

Для ведення переліку робочих системи використовується програма *Керування захистом*. Вона дозволяє виконати такі дії:

- додати робочу станцію;
- вилучити робочу станцію;
- відключити робочу станцію;
- включити робочу станцію.

Додати робочу станцію до переліку можна лише після того, як на ній була встановлена клієнтська частина системи ЛОЗА-2.

Якщо робоча станція була вилучена з переліку або відключена і клієнтська частина на ній не була деінстальована, робота за нею буде можлива лише в автономному режимі.

5 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.

Параметри, які стосуються небезпечних подій, встановлюються окремо для сервера і для кожної робочої станції (встановити одні й ті ж самі значення одночасно для в всіх комп'ютерів можна допомогою шаблона робочої станції).

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*.

6 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*.

7 Перелік скорочень та позначень

Параметри конфігурації системи захисту виділені `рівномірним шрифтом`.