Товариство з обмеженою відповідальністю
Науково-дослідний інститут
«Автопром»

Система захисту інформації

ЛОЗА™-1

версія 4.4.0

ІНСТРУКЦІЯ АДМІНІСТРАТОРА БЕЗПЕКИ

ЛОЗА-1-4.І3.01.1

ТОВ НДІ “Автопром”
Київ, 2020

Зміст

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 технологічної інформації КЗЗ – бази облікових записів, переліку рівнів доступу та даних про об’єкти захисту;

– налаштування 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, версія 4, документ може бути доповнений.

Адміністратор безпеки повинен мати базові навички роботи з операційною системою Microsoft Windows, а також розуміти основи функціонування системи ЛОЗА-1, версія 4, 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 технологічної інформації КЗЗ

Для ведення технологічної інформації КЗЗ використовується програма *Керування захистом*.

1.1 Ведення бази облікових записів

База облікових записів містить перелік користувачів системи з їхніми атрибутами доступу та перелік груп користувачів.

1.1.1 Облікові записи користувачів

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.

1.1.2 Ключові диски

У випадку, коли один з параметрів, наведених в п. 1.1.1, має значення *Так*, робота користувача за комп'ютером можлива тільки за наявності ключового диска. Ключовий диск користувача створює адміністратор. Ключовий диск можна ініціалізувати або запам'ятати (якщо він був ініціалізований раніше).

Як ключові диски можуть використовуватись дискети, знімні диски USB Flash, CD/DVD- диски та електронні ключі «Кристал-1».

CD/DVD-диски можуть бути ініціалізовані за допомогою програми *Керування захистом* у тому випадку, якщо обладнання комп'ютера дозволяє запис на такий диск. CD/DVD-диск, який має стати ключовим диском користувача, повинен бути не ініціалізованим. В іншому випадку програма дозволяє видалити наявну на ньому інформацію та підготувати до повторного запису (якщо диск є перезаписуваним). Після ініціалізації ключового диску він фіналізується, тобто стає недоступним для подальшого запису інформації на ньому. Ім'я диску задається при його ініціалізації. За умовчанням – це <Ім'я користувача>CDKey, але не більше 16-ти символів. Його можна змінити перед початком ініціалізації. На диск, крім ключа, записується службова інформація. Якщо обладнання не дозволяє записувати CD/DVD-диски, то можна записати ключ на іншому комп'ютері та запам'ятати диск як існуючий.

Для цього необхідно запустити утиліту %LOZA%\Lib\LOZAKeygen.exe, яка створює файл %LOZA%\Lib\LOZAKey.dsk. Цей файл за допомогою знімного носія, дозволеного системою, треба перенести на інший комп'ютер та за допомогою будь-якого засобу запису CD/DVD-дисків перенести на диск. Після цього диск може бути запам'ятований як ключовий. Файл LOZAKey.dsk слід видалити – для підготовки наступного диска необхідно буде створити новий файл.

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 (у тому числі CD/DVD-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.

Якщо в якості ключового диска користувача (для конфігурації *Підвищена безпека*) використовується диск USB Flash, він повинен пройти інструментальний контроль. Цей диск не дозволяється використовувати для зберігання інформації, що має гриф обмеження доступу.

1.1.3 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 прикладу.

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.sdt*.

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.sdt (*якщо файл було отримано на ранніх версіях і він має cds - формат, то його потрібно перетворити у *.sdt* і для цього потрібно використати спеціальну утиліту для перетворення*)*;

– 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*).

1.1.4 Групи користувачів

Для спрощення керування доступом та аудитом використовуються групи користувачів.

В системі визначаються два типи груп: звичайні та вбудовані. Звичайні групи можуть бути створені та видалені, до кожної з них можна додати будь-якого користувача, з кожної з них можна видалити будь-якого користувача. Вбудовані групи не створюються і не видаляються, приналежність користувачів до них визначається наведеними нижче правилами.

Кожна звичайна група має такі атрибути:

– ім'я (довільний рядок символів);

– SID групи – унікальний рядок символів;

– опис (довільний рядок символів);

– перелік облікових записів користувачів – членів групи; тут зберігається перелік SID'ів користувачів.

1.2 Ведення переліку рівнів доступу

Для встановлення рівнів допуску користувачів та рівнів доступу об'єктів захисту адміністратор безпеки має сформувати перелік рівнів доступу, які будуть використовуватись в системі. Це ті рівні доступу, які будуть відображатись у списку, що випадає при введенні рівня допуску користувача та рівнів доступу об'єктів захисту.

За умовчанням встановлюються такі значення:

- цілком таємна інформація;
- таємна інформація;
- службова інформація;
- конфіденційна інформація;
- відкрита інформація.

За допомогою програми *Керування захистом* (пункт меню *Дані – Рівні доступу*) адміністратор може відмінити використання рівнів доступу, які не будуть використовуватись в системі, або встановити додаткові рівні доступу.

1.3 Ведення даних про об'єкти захисту

1.3.1 Захищені папки

Захищеною може бути призначена будь-яка папка, яка знаходиться на жорсткому диску. Для кожної папки визначаються два види доступу – читання та запис.

У таблиці 1.1 перелічені атрибути захищених папок і вказані їхні початкові значення. Всі наведені атрибути є атрибутами доступу. Значення всіх атрибутів вказує адміністратор, який додає папку до переліку захищених папок.

Таблиця 1.1 – Атрибути захищеної папки

Назва	Пояснення
Ім'я	Повний шлях до папки
Серійний номер	Зберігається серійний номер диска, на якому знаходиться папка. Використовується номер, який не може бути змінений програмно і однозначно ідентифікує диск
Обмеження для процесів	Значення обирається з такого переліку: – так; – ні
Список процесів	Перелік дозволених процесів
Рівень доступу	Значення обирається з рівнів доступу, відмічених для використання у переліку рівнів доступу
Список доступу	Значення визначається переліком елементів такого вигляду: <користувач або група> – <вид доступу> – <дозвіл/заборона>
Список аудиту	Значення визначається переліком елементів такого вигляду: <користувач або група> – <вид доступу> – <види аудиту>.

Для кожної захищеної папки за рахунок встановлення значення *Так* для атрибута *Обмеження для процесів* можна дозволити користувачам працювати з захищеними папками та файлами, які знаходяться в них, тільки за допомогою процесів,

зазначених в атрибуті ***Список процесів***. У цьому списку вказуються шляхи до файлів, що виконуються.

1.3.2 Захищені процеси

До списку захищених процесів може належати будь-який модуль операційної системи, що виконується: файли *.exe, *.dll, *.cmd, *.bat тощо.

Для захищених процесів визначається один вид доступу – запуск.

У таблиці 1.2 перелічені атрибути захищених процесів і вказані їхні початкові значення. Значення всіх атрибутів вказує адміністратор, який додає процес до переліку захищених процесів.

Таблиця 1.2 – Атрибути захищеного процесу

Назва	Пояснення
Ім’я	Шлях до відповідного файлу
Контрольна сума	Контрольна сума відповідного файлу
Список доступу	Значення визначається переліком елементів такого вигляду: <користувач або група> – <вид доступу> – <дозвіл/заборона>
Список аудиту	Значення визначається переліком елементів такого вигляду: <користувач або група> – <вид доступу> – <види аудиту>.

1.3.3 Зареєстровані диски USB Flash

Для дисків USB Flash можуть бути встановлені «індивідуальні» атрибути доступу. Для гнучких дисків та дисків CD/DVD така можливість не передбачена, оскільки не існує надійного способу ідентифікації таких дисків.

Для зареєстрованих дисків USB Flash визначаються два види доступу – читання та запис.

Для того щоб встановити атрибути доступу для диска USB Flash, його необхідно додати до списку зареєстрованих дисків. Кожний зареєстрований диск USB Flash має атрибути, наведені у таблиці 1.3. Значення всіх атрибутів вказує адміністратор, який додає диск до переліку зареєстрованих дисків.

Таблиця 1.3 – Атрибути зареєстрованого диска USB Flash

Назва	Пояснення
Серійний номер	Зберігається так званий код екземпляру пристрою, який не може бути змінений програмно і однозначно ідентифікує диск
Обмеження для процесів	Значення обирається з такого переліку: – так; – ні
Список процесів	Перелік дозволених процесів
Рівень доступу	Значення обирається з рівнів доступу, відмічених для використання у переліку рівнів доступу

Назва	Пояснення
Список доступу	Значення визначається переліком елементів такого вигляду: <користувач або група> – <вид доступу> – <дозвіл/заборона>
Список аудиту	Значення визначається переліком елементів такого вигляду: <користувач або група> – <вид доступу> – <види аудиту>.
Довільні атрибути	Атрибути, які визначені шаблоном користувача і мають довідкове значення

Атрибути *Обмеження для процесів* та *Список процесів* використовуються так само, як і для захищених папок.

Дозволи та аудит, встановлені для зареєстрованих дисків USB Flash, мають пріоритет перед установками політики для дисків USB Flash (див. п. 1.5.6).

1.4 Архівування та відновлення бази облікових записів та даних про об'єкти захисту

Адміністратор безпеки повинен періодично виконувати архівування бази облікових записів та даних про об'єкти захисту. Орієнтовна періодичність архівування – один раз на місяць, але, якщо після останнього архівування зміни не вносились, чергове архівування не потрібне.

База облікових записів складається з двох таблиць – переліку користувачів та переліку груп користувачів. Вони містяться у службовому файлі Subjects.sqlite.

Дані про об'єкти захисту складаються з трьох таблиць – переліку захищених папок, переліку зареєстрованих дисків USB Flash та переліку захищених процесів. Вони містяться у службовому файлі Objects.sqlite.

Саме вказані переліки і треба архівувати. Для цього за допомогою програми *Керування захистом* відповідні переліки необхідно експортувати. Файли, які буде отримано в результаті експорту, і є резервними копіями.

У разі необхідності відновлення з резервної копії за допомогою програми *Керування захистом* слід імпортувати відповідну резервну копію.

Слід пам'ятати, що імпортувати переліки облікових записів можна лише у стані відновлення. Після імпорту рекомендується змінити пароль адміністратора безпеки та звірити усі списки, що імпортувалися. Імпорт відбувається без аналізу на відповідність стану цих даних в операційній системі і вони можуть частково втратити актуальність.

1.5 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:

– диски для зберігання документів;

- дозволи на доступ до технологічної інформації;
- заборонені програми;
- небезпечні команди;
- параметри входу до системи;
- параметри журналу;
- параметри заборони друку;
- параметри захисту друку та експорту документів;
- параметри перевірки цілісності;
- політики знімних дисків;
- параметри розпорядку роботи;
- переліки шаблонів та надбудов;
- політика аудиту;
- політика блокування облікового запису;
- політика паролів;
- тимчасові файли.

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

Нижче наведені докладні пояснення щодо встановлення значень цих параметрів конфігурації.

1.5.1 Встановлення дозволів на доступ до технологічної інформації

Дозволи на доступ до даних захисту визначаються параметром конфігурації системи `дозволи на доступ до технологічної інформації`. 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 облікових записів та даних про об’єкти захисту;
- параметрів конфігурації системи;
- оперативних даних про роботу системи;
- журналу реєстрації.

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 технологічної інформації` необхідно лише в особливих випадках.

1.5.2 Встановлення параметрів входу до системи

Порядок входу користувачів до системи визначається такими параметрами конфігурації:

- `відображати ім'я попереднього користувача`;
- `перевіряти ключовий диск під час входу до Windows`.

Додаткові обмеження на роботу користувачів системи можна встановити за допомогою параметра перевіряти ключовий диск під час роботи у Windows.

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

Звичайні користувачі та адміністратори документів можуть увійти до Windows тільки під час перебування системи ЛОЗА-1 в робочому стані.

Після встановлення системи ЛОЗА-1 на роботу користувачів у Windows накладаються деякі (незначні) обмеження:

– увійти до Windows зможуть тільки користувачі, які мають обліковий запис у системі ЛОЗА-1;

– замість стандартних діалогів входу до Windows, виходу з Windows, 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.

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.

Параметр відображати ім'я попереднього користувача впливає на екран входу до системи. Він визначає, чи відображається на екрані перелік користувачів системи.

Передбачена також можливість видавати користувачеві при вході в систему попередження, що стосується особливостей роботи з інформацією обмеженого доступу. Для цього використовуються параметри:

– виводити попередження при вході до системи;

– текст попередження при вході до системи.

1.5.3 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;

– мінімальний рівень доступу для використання пароля на друк документів;

– пароль на друк документів.

Надання параметру конфігурації захищати друк документів паролем значення *Так* означає, що користувач отримуватиме доступ на друк документа, рівень доступу якого не нижчий за значення параметра мінімальний рівень доступу для використання пароля на друк документів, 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;
- мінімальний рівень доступу для використання пароля на експорт документів;
- пароль на експорт документів.

1.5.4 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) 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 папки LOZADoc на фіксованому диску встановлюються ті ж дозволи на доступ, що і для папки %LOZA%\Doc. Це унеможливлює доступ до папки для всіх користувачів системи. Незмінність встановлених дозволів перевіряється під час перевірки цілісності файлів та папок.

1.5.5 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`;
– `спеціальні налаштування`.

Якщо параметр `спосіб заборони друку` має значення `спеціальні налаштування`, 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 параметр `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 параметр `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***).

1.5.6 Встановлення політик знімних дисків

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

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

Кожна політика містить список доступу та список аудиту і розповсюджується на всі диски відповідного типу.

1.5.7 Встановлення політики аудиту

Політика аудиту визначається одноіменним параметром конфігурації системи (параметр `політика аудиту`) визначає, які саме дії користувачів можуть бути зареєстровані в журналі реєстрації. Політика аудиту 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).

Встановлення аудиту для всіх категорій призводить безпосередньо до реєстрації відповідних подій у журналі.

Політика аудиту може бути встановлена досить диференційовано. Для параметрів конфігурації аудит може бути встановлений окремо для різних груп параметрів.

Значення ***за умовчанням*** політики аудиту обрано таким чином, щоб у журналі реєструвались всі події, важливі з точки зору захисту інформації, а, з іншого боку, не 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).

1.5.8 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 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.

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

1.5.9 Встановлення політики документів

Політика документів встановлює декілька загальних обмежень на роботу з документами. Вона визначається такими параметрами конфігурації системи:

– обмеження для адміністратора документів;

– дозволяти створення довірчих баз;

– максимальний рівень доступу для довірчих баз;

– реєструвати події для довірчих баз;

– примусове маркування документів перед друком;

– мінімальний рівень доступу для примусового маркування документів;

– запитувати обліковий номер документа перед друком;

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

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

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

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.

Якщо параметр конфігурації реєстрація подій для довірчих баз має значення ***Ні***, для баз із довірчим керуванням доступом аудит не 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.

Якщо параметр конфігурації запитувати обліковий номер документа перед друком має значення ***Так***, перед друком буде запитуватись обліковий номер документа.

Параметр конфігурації мінімальний рівень доступу, для якого запитується обліковий номер документа перед друком визначає мінімальний рівень доступу документів, перед друком яких буде запитуватись обліковий номер документа.

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

1.5.10 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*.

2 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*.

3 Робота з базами документів

3.1 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*.

3.2 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 аудиту буде зазначений *Невідомий обліковий запис*. Відновити доступ можна двома описаними нижче шляхами. Для відновлення використовується програма *Захищені документи*.

1) Адміністратор безпеки згідно з п. 3 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 до бази документів*;

– в діалозі вибору файлу обрати копію бази даних захисту з попередньої інсталяції.

Список користувачів може бути збережений також за допомогою програми Захищені документи. Для цього використовується пункт головного меню *База – зберегти список користувачів.* Цю дію може виконати адміністратор безпеки або адміністратор документів.

3.3 Відновлення пошкоджених баз 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 відмовостійкості, збої програмного чи апаратного забезпечення можуть призвести до пошкодження цих файлів. Для відновлення службових файлів потрібно використати пункт головного меню *База – створити/відновити базу по документах* програми *Захищені документи*. Цю дію може виконати тільки адміністратор документів. Службові файли будуть відновлені з інформації, що міститься в самих файлах. Частково дані будуть взяті за умовчанням або із запиту до користувача.

3.4 Резервне копіювання баз документів

Для забезпечення можливості відновлення баз документів у випадку збоїв необхідно регулярно виконувати резервне копіювання. Для зберігання резервних копій рекомендується використовувати окремий носій. Застосовувати програми-архіватори для економії місця на цьому носії недоцільно, оскільки документи зберігаються у системі ЛОЗА-1 у архівованому вигляді.

Всі бази документів зберігаються в кореневій директорії відповідного диска у папці LOZADoc. Для того, щоб виконати резервне копіювання, систему ЛОЗА-1 необхідно перевести у стан відновлення. У тому випадку, коли база документів зберігається на жорсткому диску, треба перед копіюванням за допомогою програми *Помічник адміністратора* (%LOZA%\AdminAssistant.exe) дозволити доступ до баз документів (на сторінці *Бази документів* натиснути кнопку *Дозволити доступ*). Після закінчення резервного копіювання треба за допомогою цієї ж програми заборонити доступ до баз документів (на сторінці *Бази документів* натиснути кнопку *Заборонити доступ*).

Перелік скорочень та позначень

%LOZA% – коренева папка системи.

Параметри конфігурації системи захисту виділено рівномірним шрифтом.