Товариство з обмеженою відповідальністю
Науково-дослідний інститут
”Автопром”

Система захисту інформації

ЛОЗА™-2

версія 4.2.0

ЗАГАЛЬНИЙ ОПИС СИСТЕМИ

ЛОЗА-2-4.ПД.01.1

ТОВ НДІ “Автопром”
Київ, 2015

Зміст

1 Призначення системи

Система ЛОЗА-2 – це комплекс програмних засобів, призначений для захисту від несанкціонованого доступу інформації, яка циркулює в локальній обчислювальній мережі (ЛОМ).

Система ЛОЗА-2 орієнтована на захист інформації, що міститься в текстових документах та електронних таблицях. Система також забезпечує захист будь-яких інших даних – на рівні папки операційної системи для даних, які зберігаються на жорсткому диску, та на рівні розділу диска – для даних які зберігаються на знімних дисках. Крім цього, до складу системи входять всі засоби, необхідні для створення комплексної системи захисту інформації від несанкціонованого доступу в інформаційно-телекомунікаційних системах .

Система випускається у двох конфігураціях: «Підвищена безпека» та «Стандартна безпека». Перша з них реалізує більш жорстку політику безпеки інформації.

Згідно з термінологією, введеною в документі НД ТЗІ 2.5-004-99. “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, система ЛОЗА-2 надає послуги безпеки, зазначені в таблицях 1.1 та 1.2.

Таблиця 1.1 Профіль системи ЛОЗА-2, конфігурація «Підвищена безпека»

Назва послуги	Рівень надання послуги	
	Позначення	Назва
Конфіденційність		
Адміністративна конфіденційність	КА-3	Повна адміністративна конфіденційність
Повторне використання об’єктів	КО-1	Повторне використання об’єктів
Цілісність		
Адміністративна цілісність	ЦА-1	Мінімальна адміністративна цілісність
Доступність		
Стійкість до відмов	ДС-1	Стійкість при обмежених відмовах
Гаряча заміна	ДЗ-1	Модернізація
Відновлення після збоїв	ДВ-1	Ручне відновлення
Спостереженість		
Реєстрація	НР-4	Детальна реєстрація
Ідентифікація та автентифікація	НИ-3	Множинна ідентифікація і автентифікація
Достовірний канал	НК-1	Однонаправлений достовірний канал
Розподіл обов’язків	НО-2	Розподіл обов’язків адміністраторів
Цілісність комплексу засобів захисту	НЦ-2	КЗЗ з гарантованою цілісністю

Назва послуги	Рівень надання послуги	
	Позначення	Назва
Самотестування	НТ-2	Самотестування при старті

Таблиця 1 . 2 Профіль системи ЛОЗА-2, конфігурація «Стандартна безпека»

Назва послуги	Рівень надання послуги	
	Позначення	Назва
Конфіденційність		
Довірча конфіденційність	КД-2	Базова довірча конфіденційність
Адміністративна конфіденційність	КА-2	Базова адміністративна конфіденційність
Повторне використання об’єктів	КО-1	Повторне використання об’єктів
Цілісність		
Довірча цілісність	ЦД-1	Мінімальна довірча цілісність
Адміністративна цілісність	ЦА-1	Мінімальна адміністративна цілісність
Доступність		
Стійкість до відмов	ДС-1	Стійкість при обмежених відмовах
Гаряча заміна	ДЗ-1	Модернізація
Відновлення після збоїв	ДВ-1	Ручне відновлення
Спостереженість		
Реєстрація	НР-4	Детальна реєстрація
Ідентифікація та автентифікація	НИ-2/НИ-3*	Одиночна ідентифікація і автентифікація/ Множинна ідентифікація і автентифікація
Достовірний канал	НК-1	Однонаправлений достовірний канал
Розподіл обов’язків	НО-2	Розподіл обов’язків адміністраторів
Цілісність комплексу засобів захисту	НЦ-2	КЗЗ з гарантованою цілісністю
Самотестування	НТ-2	Самотестування при старті

*НИ-2/НИ-3 – рівень надання послуги залежить від значень параметрів конфігурації системи ЛОЗА-2.

Під час роботи з текстовими документами та електронними таблицями користувачі системи отримують інтерфейс та можливості програм Microsoft Word та Microsoft Excel відповідно.

Текстові документи та електронні таблиці можуть зберігатись на знімних та на стаціонарних носіях (жорстких дисках).

2 Умови використання системи

Серверна та клієнтська частини системи ЛОЗА-2 можуть працювати на комп'ютері, на якому встановлена будь-яка із нижченаведених операційних систем:

- Microsoft Windows XP Professional, Service Pack 2 або вище (32-бітна версія);
- Microsoft Windows Vista, Service Pack 2 або вище (32- або 64-бітна версія);
- Microsoft Windows 7 Professional/Enterprise/Ultimate (32- або 64-бітна версія);
- Microsoft Windows 8 (32- або 64-бітна версія);
- Microsoft Windows 8.1 (32- або 64-бітна версія);
- Microsoft Windows 10 (32- або 64-бітна версія);
- Microsoft Windows Server 2003 (32-бітна або 64-бітна версія);
- Microsoft Windows Server 2008 (32- або 64-бітна версія);
- Microsoft Windows Server 2008 R2 (64-бітна версія);
- Microsoft Windows Server 2012 (64-бітна версія).
- Microsoft Windows Server 2012 R2 (64-бітна версія).

Система ЛОЗА-2 може працювати як в одноранговій мережі, так і в мережі, побудованій на основі домену.

Один із комп'ютерів мережі повинен виконувати роль сервера системи ЛОЗА-2. Надалі називатимемо його *сервером*.

В одноранговій мережі серверна частина системи ЛОЗА-2 може бути встановлена на будь-якому з комп'ютерів мережі. В мережі, побудованій на основі домену, серверна частина системи ЛОЗА-2 встановлюється на первинному контролері домену.

На всіх інших комп'ютерах встановлюється клієнтська частина системи ЛОЗА-2. Надалі називатимемо їх *робочими станціями*.

Надалі в тексті документа використовуватиметься також слово *система*, яке в залежності від контексту може позначати серверну частину системи ЛОЗА-2, клієнтську частину системи ЛОЗА-2 або стосуватись одночасно серверної та клієнтської частини системи ЛОЗА-2.

Систему ЛОЗА-2 необхідно встановлювати на диск із файловою системою NTFS.

На всіх комп'ютерах, на яких користувачі працюватимуть з документами, мають бути встановлені Microsoft Word та Microsoft Excel однієї з таких версій (32- або 64-бітна версія):

- Microsoft Office 2003;
- Microsoft Office 2007 (SP-2 або вище);
- Microsoft Office 2010;
- Microsoft Office 2013.

Разом із програмами Microsoft Word та Microsoft Excel має бути встановлена компонента відповідної версії Microsoft Office *Общие средства Office\Visual Basic для приложений*.

На комп'ютері, на якому використовується система ЛОЗА-2, має бути встановлена тільки одна операційна система, а завантаження операційної системи зі знімних дисків необхідно унеможливити за допомогою утиліти *CMOS SETUP UTILITY* (або аналогічної).

Якщо з якоїсь причини на комп'ютері все ж необхідно використовувати додаткову операційну систему, її завантаження має бути повністю контрольованим адміністратором.

3 Порядок роботи системи

3.1 Параметри конфігурації

Порядок роботи системи ЛОЗА-2 залежить від значень параметрів конфігурації, повний перелік яких наведений у Додатку А. Для зміни значень параметрів конфігурації використовується програма *Керування захистом* (пункт меню *Конфігурація*). Далі в тексті документа параметри конфігурації виділені *рівномірним шрифтом*.

Параметри конфігурації поділяються на дві групи – *загальні параметри* і *параметри комп'ютера*. Загальні параметри стосуються системи в цілому, параметри комп'ютера встановлюються окремо для кожного комп'ютера мережі (у тому числі для сервера). Таким чином, в системі одночасно зберігаються один набір загальних параметрів і декілька наборів параметрів комп'ютера – один для сервера і по одному для кожної робочої станції.

Розподіл параметрів по групах та їхні ідентифікатори наведені в таблиці А.9 додатку А.

Для зручності керування робочими станціями передбачений *шаблон робочої станції*. За допомогою шаблона можна встановити значення параметрів конфігурації для всіх робочих станцій одночасно.

Шаблон містить значення для всіх параметрів конфігурації, які належать до групи *параметри комп'ютера*. Застосування шаблона визначається параметром конфігурації *застосування шаблона робочої станції*. Він містить перелік ідентифікаторів параметрів конфігурації з групи *параметри комп'ютера*. Якщо параметр конфігурації зазначений у переліку, для всіх робочих станцій застосовується значення із шаблона.

Шаблон робочої станції не застосовується до сервера.

Одразу після інсталяції системи параметри конфігурації набувають значень за умовчанням. Передбачено два набори значень за умовчанням, а система ЛОЗА-2 може, відповідно, постачатись у двох конфігураціях: „Стандартна безпека" та „Підвищена безпека". Значення за умовчанням для обох конфігурацій наведені в таблиці А.1 Додатка А. Окрім значень за умовчанням, конфігурація „Підвищена безпека" відрізняється обмеженнями на можливі значення деяких параметрів. Відповідні відомості наведені в таблиці А.1 Додатка А.

3.2 Стани системи

Серверна та клієнтські частини системи ЛОЗА-2 можуть (незалежно) перебувати в одному з таких станів:

- робочий стан;
- стан відновлення.

Вважається, що система ЛОЗА-2 у цілому перебуває в тому ж стані, в якому знаходиться її серверна частина.

Звичайні користувачі та адміністратори документів мають доступ до даних лише в тому випадку, коли серверна та відповідна клієнтська частина системи (тобто клієнтська частина, встановлена на комп'ютері, за яким працює користувач) знаходяться в робочому стані. Цей стан призначений для проведення звичайної роботи системи і в ньому комп'ютери мають перебувати переважну частину часу.

Стан *відновлення* призначений для проведення відновлення програмного забезпечення та критичних для роботи системи даних, таких як, наприклад, системний реєстр та технологічна інформація.

Сеансом роботи називається проміжок часу між початком та наступним закінченням роботи системи.

На початку роботи система автоматично переходить у стан, який визначається за правилами, викладеними в п. 3.3. Правила завершення роботи наведені нижче в п. 3.4.

Переходи між переліченими вище станами здійснює адміністратор безпеки та/або системний адміністратор за допомогою програми *Монітор захисту*. Система може змінити стан "за власною ініціативою" лише в одному випадку – після виявлення порушень цілісності (див. п. 5.1).

Під час перебування системи в робочому стані виконується автоматична перевірка цілісності програмного середовища (див п. 5). У стані відновлення перевірка припиняється.

Під час переходу зі стану відновлення в робочий стан проводиться перевірка цілісності, і перехід здійснюється лише у випадку позитивного результату перевірки.

Вихід та вхід користувачів в операційну систему (*logon* та *logoff*) не впливають на стан системи.

3.3 Початок роботи

На кожному комп'ютері система ЛОЗА-2 починає роботу під час завантаження операційної системи. Стан, у якому починається робота системи, називається *початковим*. Вибір початкового стану відбувається за такими правилами:

а) Якщо в попередньому сеансі роботи відбулось аварійне завершення роботи, система починає роботу в стані відновлення.

б) Якщо в попередньому сеансі роботи відбулось звичайне або некоректне завершення роботи, діють наведені нижче правила.

1) Якщо параметр конфігурації *за можливості починати роботу в робочому стані* має значення *Так*, початковим станом є робочий стан.

2) Якщо параметр конфігурації *за можливості починати роботу в робочому стані* має значення *Ні,* початковим станом є стан, у якому система перебувала під час завершення роботи в попередньому сеансі.

Додатково діє таке обмеження:

в) Якщо операційна система працює в безпечному режимі (safe mode), початковим станом є стан відновлення. Вихід зі стану відновлення під час роботи в безпечному режимі не дозволяється.

3.4 Завершення роботи

Завершення роботи серверної та клієнтської частин може бути звичайним, аварійним або некоректним.

Вважається, що відбулось *звичайне* завершення роботи, якщо було здійснене завершення роботи стандартними засобами операційної системи (ОС).

У разі виявлення порушення цілісності під час перебування серверної чи клієнтської частини в робочому стані, здійснюється *аварійне* завершення роботи (якщо це визначено параметром конфігурації *реакція на порушення цілісності* – п. 5.1).

Під час аварійного завершення роботи користувач, який працює за комп'ютером, впродовж часу, що визначається параметром конфігурації *тривалість видачі попереджень про аварійне завершення роботи*, отримує попередження про необхідність закінчити роботу. Після того, як зазначений

час мине (або користувач припинить роботу), ініціюється завершення роботи операційної системи.

Якщо робота була завершена внаслідок збою або вимкнення комп'ютера, вважається, що система завершила роботу *некоректно*.

3.5 Операції

Під час роботи система автоматично виконує певні дії. Ці дії можуть бути зумовлені командами адміністратора (наприклад, адміністратор може дати команду змінити стан системи за допомогою програми *Монітор захисту*) або іншими причинами (наприклад, на початку роботи необхідно виконати перевірку цілісності).

Для зручності групи з декількох логічно пов'язаних між собою дій поєднуються в *операції* (деякі операції складаються з однієї дії). Наприклад, під час роботи системи можуть виконуватись такі операції:

- видалення тимчасових файлів;
- перевірка цілісності файлів та папок;
- перевірка безпеки середовища;
- створення файлу звіту про небезпечні події тощо.

3.6 Обробка помилок

Під час роботи ядра системи можливе виникнення різноманітних помилок, таких як відсутність параметра реєстру, неможливість доступу до файлу тощо. У цьому випадку відповідна інформація реєструється в журналі прикладних програм Windows, і система певним чином реагує на помилку.

Порядок роботи системи після виявлення помилки залежить від того, коли була виявлена помилка.

а) Якщо помилка була виявлена під час відпрацювання ядром системи запиту, який надійшов від іншої програми, ця програма отримує повідомлення про виникнення внутрішньої помилки системи захисту і має відреагувати на нього відповідним чином.

Наприклад, аудит доступу до документів здійснюється за запитом програми *Захищені документи*. У випадку виникнення помилки під час здійснення аудиту програма отримує повідомлення про помилку і виводить його на екран, а доступ до документа користувачеві не надається.

б) Якщо виявлена помилка унеможливила автоматичну перевірку цілісності під час перебування системи в робочому стані, вважається, що була порушена цілісність, і подальша поведінка системи визначається правилами, викладеними в п. 5.1.

в) Якщо помилка була виявлена під час виконання однієї з визначених у системі операцій (п. 3.5), виконання операції припиняється і в головному вікні програми *Монітор захисту* з'являється повідомлення про виникнення помилки. Якщо адміністратор у поточний момент не працює із програмою *Монітор захисту*, він отримає це повідомлення одразу після запуску програми.

У випадку, який описано в пункті в), адміністратор за допомогою програми *Монітор захисту* може спробувати виправити помилку. Йому надається докладний опис помилки і пропонується перелік можливих варіантів продовження роботи. Цей перелік залежить від операції, під час виконання якої виникла помилка, і може містити нижченаведені пункти.

1) Повторити.

Цей пункт завжди включається до переліку й означає повторну спробу виконання операції. Його треба обирати, якщо адміністратор ужив певних заходів для виправлення помилки або вважає, що чинники, які її викликали, уже не діють.

Наприклад, якщо помилка виникла через відсутність доступу до файлу, треба відповідним чином відновити права доступу і повторити виконання операції.

2) Відмінити.

Цей пункт пропонується в тому випадку, коли виконання операції можна відмінити. Наприклад, відмінити можна прийняття змін у складі програмного середовища або видалення тимчасових файлів.

У деяких випадках, коли пункт ***Відмінити*** має особливий зміст, на екрані разом із повідомленням про помилку наводиться відповідне пояснення.

3) Ігнорувати.

Цей пункт з'являється в тому випадку, коли виникнення помилки можна ігнорувати. Наприклад, у разі неможливості прочитати значення параметра конфігурації можна використати значення за умовчанням.

Якщо пункт ***Ігнорувати*** включений до переліку, на екрані разом із повідомленням про помилку наводиться відповідне пояснення.

4) Стан відновлення.

Цей пункт завжди включається до переліку й означає перехід у стан відновлення. Його треба вибирати в тому випадку, коли для виправлення помилки необхідно перевести систему в стан відновлення.

3.7 Поведінка системи

Згідно із правилами, викладеними в пп. 3.2 – 3.4, у кожний момент часу система може починати роботу, завершувати роботу або знаходитись у певному стані. Відповідна характеристика називається ***режимом роботи***. Режим роботи системи може набувати таких значень:

- початок роботи;
- перебування в певному стані;
- зміна стану;
- очікування перед виходом із стану (перед виходом із стану система чекає, доки користувач закінчить роботу);
- здійснення звичайного завершення роботи;
- здійснення аварійного завершення роботи.

Для того щоб охарактеризувати поточну поведінку системи, використовується поняття ***статус***. Статус поєднує режим роботи системи та стан, в якому вона перебуває (для режимів ***перебування у певному стані*** та ***очікування перед виходом із стану***) або з якого вона виходить (для інших режимів, крім режиму ***початок роботи***). Для режиму ***початок роботи*** стан не має сенсу.

4 Керування доступом

4.1 Користувачі системи

4.1.1 Облікові записи системи ЛОЗА-2

Для кожного користувача системи за допомогою програми *Керування захистом* створюється обліковий запис. Сукупність облікових записів утворює *перелік користувачів системи*. Обліковий запис містить такі відомості:

- ім’я користувача – довільний рядок довжиною до 20 символів, який не може містити символи " / \ [ ] : ; | = , + * ? < > @, а також не може складатись тільки із крапок та пропусків;
- SID (security identifier) користувача, який співпадає з SID’ом відповідного користувача ОС (див. нижче, п. 4.1.2.1);
- повне ім’я користувача (довільний рядок символів);
- опис користувача (довільний рядок символів);
- параметри (вони можуть бути включені або відключені):
  - вимагати зміну пароля при наступному вході до системи;
  - відключити обліковий запис;
  - заблокувати обліковий запис (адміністратор може лише розблокувати обліковий запис, блокує його тільки система);
- пароль (довільний рядок довжиною до 127 символів);
- ролі користувача (п. 4.1.1.1);
- рівень доступу користувача (п. 4.1.1.2);
- відомості про ключовий диск (ключові диски) користувача (п. 4.1.3).

Під час створення облікового запису рекомендується встановити вимогу зміни пароля при наступному вході до системи. Користувач повинен буде змінити пароль при першій же реєстрації у системі і, таким чином, свій пароль знатиме тільки сам користувач.

Якщо обліковий запис відключений або заблокований, користувач не зможе ввійти до системи. Заблокувати обліковий запис може тільки система (п. 4.1.4.2), адміністратор не має такої можливості.

Відповідність між обліковими записами системи ЛОЗА-2 та обліковими записами Windows описана нижче, у п. 4.1.2.1.

4.1.1.1 Ролі користувачів

Для забезпечення можливості розподілу обов’язків у системі визначені такі ролі користувачів:

- *Звичайний користувач*;
- *Адміністратор безпеки*;
- *Адміністратор документів*;
- *Системний адміністратор*.

Останні три ролі називатимемо *адміністративними*.

Роль *Звичайний користувач* не суміщається з жодною з адміністративних ролей; адміністративні ролі можна суміщати будь-яким чином.

Далі в тексті документа “адміністратор безпеки” позначає особу або групу осіб, які виконують роль *Адміністратор безпеки*. Аналогічним чином здійснюється посилання на інші адміністративні ролі. Терміном “адміністратор” позначається особа, якій встановлена роль *Адміністратор безпеки* або роль *Системний адміністратор*.

4.1.1.2 Рівень доступу користувача

Рівень доступу обирається з ієрархічного набору значень, який складає *перелік рівнів доступу*. Коригувати цей перелік можна за допомогою програми *Керування захистом.* Перелік рівнів доступу складається з 25 елементів, кожний з яких має такі атрибути:

– використання – логічний (булевський) атрибут, який приймає значення *Так* або *Ні* та вказує, чи використовується в системі відповідний рівень доступу;

– вид інформації – назва рівня доступу;

– гриф обмеження доступу – рядок, який використовується для маркування паперових або електронних документів під час друку або експорту.

За умовчанням перелік має вигляд, наведений у таблиці 4.1. Значення в цьому переліку розташовані за спаданням, перше вважається найвищим, останнє – найнижчим.

Таблиця 4.1 – Перелік рівнів доступу. Значення за умовчанням.

Використання	Вид інформації	Гриф обмеження доступу
Ні	Рівень 1	
Ні	Рівень 2	
Ні	Рівень 3	
Ні	Рівень 4	
Так	цілком таємна інформація	цілком таємно
Ні	Рівень 6	
Ні	Рівень 7	
Ні	Рівень 8	
Ні	Рівень 9	
Так	таємна інформація	таємно
Ні	Рівень 11	
Ні	Рівень 12	
Ні	Рівень 13	
Ні	Рівень 14	
Так	службова інформація	для службового користування
Ні	Рівень 16	
Ні	Рівень 17	
Ні	Рівень 18	
Ні	Рівень 19	
Так	конфіденційна інформація	конфіденційно
Ні	Рівень 21	
Ні	Рівень 22	
Ні	Рівень 23	
Ні	Рівень 24	
Так	відкрита інформація	

Таким чином, за умовчанням встановлене використання рівнів доступу інформації, визначеним законодавством України.

Рівень доступу користувача обирається з переліку рівнів доступу, серед рівнів доступу, відмічених для використання.

4.1.1.3 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, із 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.

Вбудованими є такі групи: *Адміністратори безпеки, Системні адміністратори*, *Адміністратори документів*, *Звичайні користувачі*, *Всі*, *Власник бази* та *Власник документа*.

Приналежність користувачів до вбудованих груп визначається природним чином, а саме:

– членами групи *Адміністратори безпеки, Системні адміністратори*, *Адміністратори документів* або *Звичайні користувачі* є всі користувачі системи, яким надана відповідна роль;
– членами групи *Всі* є всі користувачі системи;
– єдиним членом групи *Власник бази* є користувач – власник бази документів;
– єдиним членом групи *Власник документа* є користувач – власник документа.

Звичайно, групи *Власник бази* та *Власник документа* можуть використовуватись лише для керування доступом до документів та баз документів. Група *Власник документа* дозволяє надавати повноваження користувачу під час застосування механізму успадкування (див. п. 4.2.3.3).

Групи користувачів не мають атрибутів доступу.

4.1.2 Облікові записи Windows

4.1.2.1 Облікові записи користувачів

Кожний користувач системи ЛОЗА-2 повинен мати обліковий запис у Windows.

У мережі, побудованій на основі домену, обліковий запис створюється на первинному контролері домену. В одноранговій мережі облікові записи створюються на сервері системи ЛОЗА-2, а також на тих робочих станціях, на яких працює користувач. На робочій станції обліковий запис створюється системою ЛОЗА-2 під час входу користувача до системи.

Під час створення облікового запису в системі ЛОЗА-2 адміністратор безпеки може вибрати один з облікових записів Windows на сервері системи ЛОЗА-2 (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 у Windows. Після встановлення властивостей облікового запису системи ЛОЗА-2 встановлюються відповідні властивості облікового запису Windows.

На початку роботи та під час виходу зі стану відновлення система ЛОЗА-2 перевіряє відповідність своїх облікових записів та облікових записів Windows і в разі

виявлення розбіжностей змінює відповідні властивості облікових записів Windows. Якщо ж виявляється, що обліковий запис Windows видалений, відповідний обліковий запис видаляється з переліку користувачів системи ЛОЗА-2.

4.1.2.2 Облікові записи локальних груп

Для зручності керування повноваженнями користувачів щодо доступу до об'єктів операційної системи використовуються локальні групи Windows. Кожна група, крім групи *LOZAUsers*, відповідає певній ролі користувачів. Перелік груп та ролей, що їм відповідають, наведений у таблиці 4.1. Усі ці групи створюються під час інсталяції системи.

Таблиця 4.1

Ім'я групи	Опис групи	Роль користувача
LOZASecAdmins	Адміністратори безпеки системи ЛОЗА-2	*Адміністратор безпеки*
LOZADocAdmins	Адміністратори документів системи ЛОЗА-2	*Адміністратор документів*
LOZAOrdinaryUsers	Звичайні користувачі системи ЛОЗА-2	*Звичайний користувач*
LOZASysAdmins	Системні адміністратори системи ЛОЗА-2	*Системний адміністратор*
LOZAUsers	Усі користувачі системи ЛОЗА-2	

Під час встановлення ролей користувача за допомогою програми ***Керування захистом*** він автоматично включається до відповідних груп. Користувачі, яким надається роль ***Адміністратор безпеки*** або ***Системний адміністратор***, автоматично включаються також до вбудованої локальної групи ***Администраторы*** Windows.

Крім того, усі користувачі системи автоматично включаються до групи *LOZAUsers*.

4.1.2.3 Службові користувачі

Програми ***Сервер безпеки, Сервер документів*** та *LOZAGuard* працюють від імені певних користувачів Windows, які називаються ***службовими***. Відповідні облікові записи створюються під час інсталяції системи.

4.1.3 Ключові диски

Ключові диски використовуються для додаткової автентифікації користувачів системи (п. 4.1.5). На ключовому диску зберігається пароль користувача.

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

Для того, щоб диск став ключовим, адміністратор безпеки повинен його ініціалізувати. Під час ініціалізації на диск записується пароль, який (після подвійного хеш-перетворення) запам'ятовується в базі облікових записів.

Кожний користувач може мати два ключові диски – основний та резервний, які надають йому однакові повноваження. На кожному диску під час ініціалізації записується свій пароль.

4.1.4 Політика облікових записів

Політика облікових записів системи ЛОЗА-2 складається із двох груп параметрів конфігурації. Перша з них утворює політику паролів, друга – політику блокування облікового запису.

4.1.4.1 Політика паролів

Політика паролів складається з таких параметрів конфігурації:

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

Перший параметр обмежує можливість користувачів використовувати старі паролі під час зміни пароля, другий визначає термін, після закінчення якого система примушує користувача змінити пароль. Параметр *мінімальний термін дії пароля* не дозволяє користувачу змінити пароль, якщо він вже був щойно змінений і таким чином, після декількох змін повернутись до старого пароля. Параметр *мінімальна довжина пароля* не дозволяє використовувати занадто короткі паролі, а останній параметр змушує 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:

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

4.1.4.2 Політика блокування облікового запису

Політика складається із двох параметрів конфігурації:

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

Другий параметр 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.

Перший параметр визначає інтервал, після закінчення якого відлік невдалих спроб входу поновлюється.

4.1.5 Вхід 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-2 у робочому стані.

Після встановлення системи ЛОЗА-2 на роботу користувачів у Windows накладаються деякі (незначні) обмеження:

– увійти до Windows зможуть тільки користувачі, які мають обліковий запис у системі ЛОЗА-2;

– у Windows XP/2003 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-2;

– під час входу до системи користувачі будуть змушені використовувати комбінацію клавіш Ctrl+Alt+Del;

– у Windows XP/2003 буде відключена можливість запуску програм від імені іншого користувача;

– будуть відключені екран привітання Windows XP/2003 та можливість швидкого переключення між користувачами Windows XP/2003.

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. Для Windows XP/2003 він визначає, чи відображається ім'я попереднього користувача в діалозі входу до системи ЛОЗА-2. Для Windows Vista/7/8/8.1/10/2008/2012 цей параметр визначає, чи відображається на екрані перелік користувачів системи.

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.

4.1.6 Використання груп ОС

Для встановлення дозволів NTFS на доступ до підпапок папки *%LOZA%* та до папок для зберігання документів на жорсткому диску використовуються групи ОС, які створюються під час інсталяції системи ЛОЗА-2. Під час створення групам надаються певні права. Кожна група, крім групи *LOZAUsers*, відповідає деякій ролі користувача або серверної програми. Перелік груп, які створюються на сервері, ролей, що відповідають групам, та наданих їм прав наведений у таблиці 4.2.

Таблиця 4.2

Локальна група	Опис групи	Роль користувача	Права, що надаються групі
LOZASecAdmins	Адміністратори безпеки системи ЛОЗА-2	*Адміністратор безпеки*	Права не надаються

Локальна група	Опис групи	Роль користувача	Права, що надаються групі
LOZASysAdmins	Системні адміністратори системи ЛОЗА-2	*Системний адміністратор*	Права не надаються
LOZADocAdmins	Адміністратори документів системи ЛОЗА-2	*Адміністратор документів*	Права не надаються
LOZAOrdinaryUsers	Звичайні користувачі системи ЛОЗА-2	*Звичайний користувач*	Права не надаються
LOZASecServers	Сервери безпеки системи ЛОЗА-2		Вход в качестве пакетного задания (Право входити у систему як пакетне завдання)
LOZADocServers	Сервери документів системи ЛОЗА-2		Вход в качестве службы (Право входити у систему як служба)
LOZAUsers	Усі користувачі системи ЛОЗА-2		Права не надаються

Групи *LOZASecServers* та *LOZADocServers* призначені для включення до них службових користувачів, від імені яких запускаються програми *Сервер безпеки* та *Сервер документів* відповідно.

Під час встановлення ролей користувача за допомогою програми *Керування захистом* він автоматично включається до відповідних груп. Користувачі, яким надається роль *Адміністратор безпеки* або *Системний адміністратор*, автоматично включаються до локальної групи *Администраторы* Windows. До групи *Администраторы* включається також службовий користувач, від імені якого запускається *Сервер безпеки*.

Крім того, усі користувачі системи (у тому числі і службові) автоматично включаються до групи *LOZAUsers*.

Перелік груп, які створюються на робочих станціях, наведений у таблиці 4.3.

Таблиця 4.3

Локальна група	Опис групи	Роль користувача	Права, що надаються групі
LOZASecServers	Сервери безпеки системи ЛОЗА-2		Вход в качестве пакетного задания (Право входити у систему як пакетне завдання)
LOZADocServers	Сервери документів системи ЛОЗА-2		Вход в качестве службы (Право входити у систему як служба)

Групи, які відповідають ролям користувачів, на робочих станціях не створюються.

4.2 Об’єкти захисту

Система ЛОЗА-2 дозволяє захистити інформацію, яка міститься в таких об’єктах:

- бази документів.
- документи;
- захищені папки;
- знімні диски;
- захищені процеси;
- технологічна інформація:
- база облікових записів;
  - список користувачів (перелік користувачів із їхніми атрибутами доступу та даними, необхідними для автентифікації);
  - список груп користувачів;
- дані про об’єкти захисту:
  - список захищених папок;
  - список зареєстрованих дисків USB Flash;
  - список захищених процесів;
  - дані про бази документів та документи;
- перелік робочих станцій;
- журнал реєстрації;
- параметри конфігурації системи;
- оперативні дані про роботу системи (дані про поточний стан системи, результати перевірок цілісності, відомості про операції, які наразі виконуються у системі тощо).

4.2.1 Основні атрибути доступу об’єктів захисту

4.2.1.1 Рівень доступу

Частина об’єктів захисту має рівень доступу. Для всіх об’єктів рівень доступу обирається з переліку рівнів доступу (див. п 4.1.1.2), серед рівнів доступу, відмічених для використання.

4.2.1.2 Списки доступу та списки аудиту

Кожний об’єкт захисту має список доступу та список аудиту.

Список доступу – це перелік облікових записів користувачів чи груп користувачів, в якому для кожного облікового запису перелічені всі можливі види доступу до об’єкта і для кожного виду доступу вказано, дозволений цей доступ обліковому запису чи заборонений.

Список доступу можна уявляти собі як перелік елементів такого вигляду:

<користувач або група> – <вид доступу> – <дозвіл/заборона>.

Список аудиту – це перелік облікових записів користувачів чи груп користувачів, в якому для кожного облікового запису перелічені всі можливі види доступу до об’єкта і для кожного виду доступу вказано, чи потрібно реєструвати в журналі реєстрації успішні та неуспішні спроби здійснити цей вид доступу.

Список аудиту можна уявляти собі як перелік елементів такого вигляду:

<користувач або група> – <вид доступу> – <види аудиту>.

Поле *Види аудиту* може приймати значення *Аудит успіхів*, *Аудит відмов* або містити обидва ці значення.

4.2.2 Бази документів

У системі обробляються документи двох видів: текстові документи та електронні таблиці. Документи зберігаються в базах документів. В одній базі можуть зберігатись документи обох видів. Усередині бази документи можуть бути розподілені по папках.

Для кожної бази встановлюється принцип керування доступом – адміністративне або довірче керування (далі задля стислості використовуються терміни “адміністративні бази” та “довірчі бази”).

4.2.2.1 Атрибути бази

Кожна база документів має атрибути, перелічені в таблиці 4.4. Усі атрибути, крім останніх трьох, є атрибутами доступу. Початкові значення атрибутів встановлюються під час її створення.

Таблиця 4.4 – Атрибути бази документів

Назва	Пояснення	Початкове значення
Назва	Довільний рядок (довжина назви не обмежується)	Вказує користувач, який створює базу
Принцип керування доступом	Може приймати два значення: *Адміністративне керування* та *Довірче керування*	Значення встановлюється автоматично і не може бути змінене (п. 4.2.2.4)
Власник	Зберігається SID власника бази	Користувач, який створює базу
Максимальний рівень доступу документів	Значення обирається з з переліку рівнів доступу (див. п 4.1.1.2), серед рівнів доступу, відмічених для використання	Вказує користувач, який створює базу
Мінімальний рівень доступу документів	____“____	____“____
Список доступу	п. 4.1.1.2	Користувачу *Власник* встановлюється *Повний доступ* (п. 4.2.2.3)
Список аудиту	п. 4.1.1.2 Аудит подій для довірчих баз може бути заборонений політикою документів (див. п. 4.2.2.5).	Для групи *Всі* встановлюється аудит відмов для всіх видів доступу та аудит успіхів для таких видів доступу (п. 4.2.2.3): – створення документів; – запис; – керування доступом
Список доступу для документів	п. 4.1.1.2 Визначає список доступу, який успадковуються під час створення документів у базі (див. п. 4.2.3.3).	Для довірчих баз користувачу *Власник* встановлюється *Повний доступ*. Для адміністративних баз користувачу *Власник* встановлюються дозволи на такі види доступу: *коригування, друк та експорт* (п. 4.2.3.2)

Назва	Пояснення	Початкове значення
Список аудиту для документів	п. 4.1.1.2 Визначає список аудиту, який успадковуються під час створення документів у базі (див. п. 4.2.3.3). Аудит подій для довірчих баз може бути заборонений політикою документів (див. п. 4.2.2.5).	Для групи *Всі* встановлюється аудит відмов для всіх видів доступу та аудит успіхів для таких видів доступу (п. 4.2.3.2): – друк та експорт; – запис власника; – запис рівня доступу; – запис списку доступу; – запис списку аудиту
Перелік додаткових атрибутів	Додаткові атрибути, які мають документи бази, та пов'язані з цими атрибутами відомості (п. 4.2.3.1). Після створення бази значення атрибута не може бути змінене	Порожній перелік

4.2.2.2 Власник бази

Власником бази стає користувач, який створює базу.

Власником довірчої бази може бути лише звичайний користувач, власником адміністративної бази – лише адміністратор документів (п. 4.2.2.4).

4.2.2.3 Види доступу до баз

Розрізняють базові та складені види доступу. У таблиці 4.5 наведені визначені в системі базові види доступу до баз документів та необхідні пояснення.

Таблиця 4.5 – Базові види доступу до баз документів

Вид доступу	Пояснення
Читання атрибутів	Читання атрибутів бази
Читання довідників	Читання довідників бази
Читання списку документів	Читання папок, списку документів у кожній папці, всіх стандартних та додаткових атрибутів документів, а також рівня доступу кожного документа
Створення папок	
Видалення папок	
Перейменування папок	
Створення документів	
Коригування довідника типів документів	Видалення/коригування/додавання записів у довіднику типів документів
Запис атрибутів	Запис атрибутів бази, крім атрибутів *Власник*, *Список доступу* та *Список аудиту*
Запис власника	
Запис списку доступу	
Запис списку аудиту	
Перейменування	
Видалення	

Для зручності керування доступом визначаються наведені в таблиці 4.6 складені види доступу, кожний з яких є поєднанням декількох базових видів доступу.

Таблиця 4.6 – Складені види доступу до баз документів

Вид доступу	Складові
Читання	– Читання атрибутів; – Читання довідників; – Читання списку документів
Запис	– Створення папок; – Видалення папок; – Перейменування папок; – Коригування довідника типів документів; – Запис атрибутів; – Перейменування; – Видалення
Коригування	– Читання атрибутів; – Читання довідників; – Читання списку документів ; – Створення папок; – Видалення папок; – Перейменування папок; – Коригування довідника типів документів; – Запис атрибутів; – Перейменування; – Видалення
Коригування папок	– Створення папок; – Видалення папок; – Перейменування папок
Створення документів	– Створення документів
Керування доступом	– Читання атрибутів; – Читання довідників; – Читання списку документів; – Запис власника; – Запис рівня доступу; – Запис списку доступу; – Запис списку аудиту

Вид доступу	Складові
Повний доступ	– Читання атрибутів; – Читання довідників; – Читання списку документів; – Створення папок; – Видалення папок; – Перейменування папок; – Створення документів; – Коригування довідника типів документів; – Запис атрибутів; – Перейменування; – Видалення; – Запис власника; – Запис рівня доступу; – Запис списку доступу; – Запис списку аудиту

4.2.2.4 Створення баз

База документів може бути створена адміністратором документів або звичайним користувачем.

Принцип керування доступом для бази документів автоматично встановлюється під час її створення і не може бути змінений. Він визначається за таким правилом.

Якщо користувачеві, який створює базу, встановлена роль *Звичайний користувач*, для неї встановлюється довірче керування доступом.

Якщо базу створює користувач із роллю *Адміністратор документів*, для неї встановлюється адміністративне керування доступом.

4.2.2.5 Політика документів

Робота з документами регламентується декількома параметрами конфігурації системи, які утворюють *політику документів*. Ці параметри і необхідні пояснення наведені в таблиці 4.7.

Таблиця 4.7 – Політика документів

Назва	Пояснення
Обмеження для адміністратора документів	Якщо цей параметр має значення *Так*, користувачу з роллю *Адміністратор документів* під час роботи з адміністративними базами 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

Назва	Пояснення
Дозволяти створення довірчих баз	Може приймати значення *Так* та *Ні*. Встановлення значення *Ні* забороняє створення довірчих баз
Максимальний рівень доступу для довірчих баз	Значення обирається з переліку рівнів доступу (див. п 4.1.1.2), серед рівнів доступу, відмічених для використання. Для конфігурації „Підвищена безпека” цей параметр має значення *Відкрита інформація*, яке не може бути змінене. Значення цього параметра обмежує вибір значення атрибута бази *Максимальний рівень доступу документів* для всіх довірчих баз
Реєструвати події для довірчих баз	Вказує, чи здійснюється реєстрація подій для довірчих баз
Примусове маркування документів перед друком	Якщо цей параметр має значення *Так*, під час друку документів із рівнем доступу, який визначається параметром *мінімальний рівень доступу для примусового маркування документів*, до тексту документа автоматично додається гриф обмеження доступу документа (у правому верхньому куті)
Мінімальний рівень доступу для примусового маркування документів	Значення обирається з переліку рівнів доступу (див. п 4.1.1.2), серед рівнів доступу, відмічених для використання. Параметр визначає мінімальний рівень доступу документів, перед друком яких буде здійснюватись примусове маркування

4.2.3 Документи

4.2.3.1 Атрибути документів

Кожний документ має низку атрибутів. Атрибути поділяються на стандартні, додаткові та атрибути доступу.

У таблиці 4.8 перелічені стандартні атрибути документа і вказані їхні початкові значення.

Таблиця 4.8 – Стандартні атрибути документа

Назва	Пояснення	Початкове значення
Назва	Довільний рядок (довжина назви не обмежується)	Вказує користувач, який створює документ
Вид	Може приймати два значення: *Текстовий документ* та *Електронна таблиця*	——“——
Тип	Перелік типів документів визначається довідником бази документів	——“——
Тільки для читання	Може приймати два значення: *Так*, *Ні*	——“——
Ключові слова та вирази	Довільна кількість рядків довільної довжини	——“——
Коментар	Довільний текст	——“——
Код	Унікальний у межах бази документів код, який складається з восьми десяткових цифр	Встановлюється автоматично
Час створення	Дата та час створення документа	——“——

Назва	Пояснення	Початкове значення
Час останнього коригування	Дата та час останнього коригування документа	——“——

Атрибути *Вид* та *Код* встановлюються раз і назавжди, їхні значення не можуть бути змінені.

Атрибути *Час створення* та *Час останнього коригування* ведуться автоматично, їхні значення не можуть бути змінені вручну.

Окрім стандартних атрибутів, для кожної бази документів може бути визначена довільна кількість додаткових атрибутів, наприклад, *Видавник*, *Дата затвердження*, *Установа, яка затвердила документ* тощо. Для кожного додаткового атрибута встановлюються *ім'я* та *тип*. Тип додаткового атрибута може набувати таких значень: *ціле число*, *рядок*, *дата*, *дата/час*.

Перелік додаткових атрибутів встановлюється під час створення бази документів і не може бути змінений.

Таблиця 4.9 містить атрибути доступу документа і їхні початкові значення.

Таблиця 4.9 – Атрибути доступу документа

Назва	Пояснення	Початкове значення
Власник	Зберігається SID власника документа	Встановлюється автоматично. Власником стає користувач, який створив документ
Рівень доступу	Значення обирається з переліку рівнів доступу (див. п 4.1.1.2), серед рівнів доступу, відмічених для використання. Перелік обмежується атрибутами бази *Максимальний рівень доступу документів* та *Мінімальний рівень доступу документів*	Вказує користувач, який створює документ. Значення не може бути більшим, ніж рівень доступу цього користувача
Список доступу	Див. п. 4.2.1.2	Успадковується від бази (п. 4.2.3.3)
Список аудиту	Див. п. 4.2.1.2	Успадковується від бази (п. 4.2.3.3)

4.2.3.2 Види доступу до документів

Розрізняють базові та складені види доступу. У таблиці 4.10 наведені базові види доступу до документів та необхідні пояснення.

Таблиця 4.10 – Базові види доступу до документів

Вид доступу	Пояснення
Читання	Читання тексту документа або електронної таблиці

Вид доступу	Пояснення
Запис даних	Коригування тексту документа або електронної таблиці, в тому числі заміна документа (заміна вмісту документа вмістом іншого документа)
Запис стандартних та додаткових атрибутів	
Друк	
Експорт	Збереження документа у вигляді файлу (на жорсткому диску, дискеті чи іншому носії)
Видалення	
Читання атрибутів доступу[1]	Читання атрибутів *Власник*, *Список доступу*, *Список аудиту*
Запис власника	
Запис рівня доступу	
Запис списку доступу	
Запис списку аудиту	

[1]Читання атрибута *Рівень доступу* є складовою виду доступу до бази документів *Читання списку документів*.

Для зручності керування доступом визначаються наведені в таблиці 4.11 складені види доступу, кожний з яких є поєднанням декількох базових видів доступу.

Таблиця 4.11 – Складені види доступу до документів

Вид доступу	Складові
Читання	– Читання
Запис	– Запис вмісту документа; – Запис стандартних та додаткових атрибутів; – Видалення
Коригування	– Читання; – Запис вмісту документа; – Запис стандартних та додаткових атрибутів; – Видалення
Друк та експорт	– Друк; – Експорт
Коригування, друк та експорт	– Читання; – Запис вмісту документа; – Запис стандартних та додаткових атрибутів; – Видалення; – Друк; – Експорт
Керування доступом	– Читання атрибутів доступу; – Запис власника; – Запис рівня доступу; – Запис списку доступу; – Запис списку аудиту

Вид доступу	Складові
Повний доступ	– Читання; – Читання атрибутів доступу; – Запис вмісту документа; – Запис стандартних та додаткових атрибутів; – Видалення; – Друк; – Експорт; – Запис власника; – Запис рівня доступу; – Запис списку доступу; – Запис списку аудиту

4.2.3.3 Успадкування атрибутів доступу

Документ, який створюється в базі, успадковує її список доступу для документів та список аудиту для документів.

Успадковуються також ті елементи списку доступу для документів та списку аудиту для документів, які містять групу ***Власник документів***. Відповідні повноваження отримує користувач, який створює документ. Після зміни власника ці повноваження отримає новий власник.

Під час зміни списку доступу для документів та списку аудиту для документів також застосовується механізм успадкування: користувач, який змінює ці атрибути, має можливість вказати, чи треба розповсюдити зміни на всі документи бази.

4.2.4 Захищені папки

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

У таблиці 4.12 перелічені атрибути захищених папок і вказані їхні початкові значення. Усі наведені атрибути є атрибутами доступу. Значення всіх атрибутів вказує адміністратор, який додає папку до списку захищених папок.

Таблиця 4.12 – 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 процесів, за допомогою яких користувачі можуть отримати доступ до даних, які зберігаються в захищеній папці
Рівень доступу	Значення обирається з переліку, наведеного в п. 4.2.1.1

Назва	Пояснення
Список доступу	Див. п. 4.1.1.2
Список аудиту	Див. п. 4.1.1.2

Для кожної захищеної папки за рахунок встановлення значення *Так* для атрибута *Обмеження для процесів* можна дозволити користувачам працювати із 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.

4.2.5 Знімні диски

4.2.5.1 Політика знімних дисків

Для знімних дисків визначаються два види доступу – читання та запис.

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

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

Кожна політика складається з компонентів, наведених у таблиці 4.13.

Таблиця 4.13 – Політика знімних дисків

Назва	Пояснення
Список доступу	Див. п. 4.1.1.2
Список аудиту	Див. п. 4.1.1.2

Політика дисків діє одночасно на всі диски відповідного типу.

4.2.5.2 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 4.14. Значення всіх атрибутів вказує адміністратор, який додає диск до списку зареєстрованих дисків.

Таблиця 4.14 – Атрибути зареєстрованого диска USB Flash

Назва	Пояснення
Серійний номер	Зберігається так званий код екземпляра пристрою, який не може бути змінений програмно і однозначно ідентифікує диск
Обмеження для процесів	Значення обирається з такого переліку: – Так; – Ні.

Назва	Пояснення
Список процесів	Перелік процесів, за допомогою яких користувачі можуть отримати доступ до даних, які зберігаються на диску
Рівень доступу	Значення обирається з переліку, наведеного в п. 4.2.1.1
Список доступу	Див. п. 4.1.1.2
Список аудиту	Див. п. 4.1.1.2

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

4.2.6 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 4.15 перелічені атрибути захищених процесів і вказані їхні початкові значення. Значення всіх атрибутів вказує адміністратор, який додає процес до списку захищених процесів.

Таблиця 4.15 – Атрибути захищеного процесу

Назва	Пояснення
Ім’я	Шлях до відповідного файлу
Контрольна сума	Контрольна сума відповідного файлу
Список доступу	Див. п. 4.1.1.2
Список аудиту	Див. п. 4.1.1.2

4.2.7 Технологічна інформація

До технологічної інформації належать такі дані:

- база облікових записів:
  - список користувачів;
  - список груп користувачів;
- дані про об’єкти захисту:
  - список захищених папок;
  - список зареєстрованих дисків USB Flash;
  - список захищених процесів;
  - дані про бази документів та документи;
- перелік робочих станцій;
- журнал реєстрації;
- параметри конфігурації системи;
- оперативні дані про роботу системи (дані про поточний стан системи, результати перевірок цілісності, відомості про операції, які наразі виконуються у системі тощо).

Для забезпечення можливості гранульованого керування доступом до параметрів конфігурації вони розподілені на такі групи:

- 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;
– параметри розпорядку роботи;
– переліки шаблонів та надбудов;
– політика аудиту;
– політика блокування облікового запису;
– політика документів;
– політика паролів;
– політики знімних дисків;
– тимчасові файли.

Склад кожної групи наведений у Додатку А.

Для технологічної інформації визначаються два види доступу:
– читання;
– запис.

Для оперативних даних про роботу системи ***запис*** означає керування системою, – це зміни стану системи, проведення перевірок цілісності, прийняття виявлених змін, обробка помилок тощо.

4.3 Правила розмежування доступу

Довірче керування доступом застосовується до таких об’єктів:
– бази документів із довірчим керуванням доступом;
– документи з довірчим керуванням доступом.

Адміністративне керування доступом застосовується до таких об’єктів:
– бази документів з адміністративним керуванням доступом;
– документи з адміністративним керуванням доступом;
– технологічна інформація.

4.3.1 Доступ до баз документів

Всередині довірчих та адміністративних баз можуть бути створені папки, для яких є можливість створення окремих списків доступу та аудиту.

4.3.1.1 ПРД для баз із довірчим керуванням доступом

Працювати з довірчими базами можуть лише звичайні користувачі. Можливість доступу визначається списком доступу бази, її максимальним рівнем доступу, а також роллю та рівнем доступу користувача.

Користувач отримує доступ до бази документів, якщо виконуються наведені нижче умови.
– користувачу встановлена роль *Звичайний користувач*;
– рівень доступу користувача не нижчий за максимальний рівень доступу документів цієї бази;

– у списку доступу бази користувачу або групі, до якої він належить, не заборонено цей доступ;

– у списку доступу бази користувачу або групі, до якої він належить, надано цей доступ.

Власник бази має особливі повноваження щодо доступу до "своєї" бази.

Якщо користувач є власником бази і йому встановлена роль *Звичайний користувач*, він отримує до бази такі види доступу:

– читання списку документів;
– читання атрибутів;
– запис власника;
– запис списку доступу;
– запис списку аудиту.

Додатково, для того щоб не втратити можливість доступу до бази у випадку відсутності власника, а також для забезпечення можливості реалізації аналогічного додаткового правила доступу до документів (п. 4.3.2.1) встановлюється ще одне правило, яке діє для всіх довірчих баз незалежно від списку доступу бази.

Користувачі з роллю *Адміністратор безпеки* отримують такі види доступу до всіх баз:

– читання списку документів;
– читання атрибутів;
– запис власника.

4.3.1.2 ПРД для баз із адміністративним керуванням доступом

Працювати з адміністративним базами можуть звичайні користувачі та адміністратори документів. Можливість доступу визначається списком доступу бази, її максимальним рівнем доступу, а також роллю та рівнем доступу користувача.

Користувач отримує доступ до бази документів, якщо виконуються наведені нижче умови.

– йому встановлена роль *Звичайний користувач* або роль *Адміністратор документів*;

– рівень доступу користувача не нижчий за максимальний рівень доступу документів цієї бази;

– у списку доступу бази користувачу або групі, до якої він належить, не заборонено цей доступ;

– у списку доступу бази користувачу або групі, до якої він належить, надано цей доступ.

Власник бази має особливі повноваження щодо доступу до "своєї" бази, які діють незалежно від списку доступу бази.

Якщо користувач є власником бази і йому встановлена роль *Адміністратор документів*, він отримує до бази такі види доступу:

– читання списку документів;
– читання атрибутів;
– запис власника;
– запис списку доступу;
– запис списку аудиту.

Крім цього, для адміністративних баз встановлюються обмеження, які не дозволяють звичайним користувачам керувати доступом до баз. Ці обмеження діють незалежно від списку доступу бази.

Звичайні користувачі не можуть отримати такі види доступу до бази документів:
- запис атрибутів;
- зміна назви;
- видалення;
- запис власника;
- запис списку доступу;
- запис списку аудиту.

Якщо параметр політики документів (п. 4.2.2.5) *Обмеження для адміністратора документів* має значення *Так*, користувачі, яким встановлена роль *Адміністратор документів*, не можуть отримати до бази документів доступ на створення документів.

Користувачі, яким встановлена роль *Адміністратор документів* та роль *Адміністратор безпеки* або *Системний адміністратор*, не можуть отримати до бази документів доступ на створення документів.

Для того, щоб не втратити можливість доступу до бази у випадку відсутності власника, встановлюється ще одне правило.

Користувачі з роллю *Адміністратор безпеки* отримують такі види доступу до всіх баз:
- читання списку документів;
- читання атрибутів;
- запис власника.

4.3.2 Доступ до документів

Правила розмежування доступу (ПРД) до документа залежать від принципу керування доступом, встановленого для бази, у якій міститься документ.

4.3.2.1 ПРД для баз із довірчим керуванням доступом

У довірчих базах працювати з документами можуть лише звичайні користувачі. Можливість доступу визначається списком доступу документа, його рівнем доступу, а також роллю та рівнем доступу користувача.

Користувач отримує доступ до документа, якщо виконуються наведені нижче умови.
- рівень доступу користувача не нижчий за рівень доступу документа;
- йому встановлена роль *Звичайний користувач*;
- у списку доступу документа користувачу або групі, до якої він належить, не заборонено цей доступ;
- у списку доступу документа користувачу або групі, до якої він належить, надано цей доступ.

Власник документа має особливі повноваження щодо доступу до “своїх” документів, які діють незалежно від списку доступу документа.

Якщо користувачу встановлена роль *Звичайний користувач*, він є власником документа і його рівень доступу не нижчий за рівень доступу документа, він отримує до документа такі види доступу:

- читання атрибутів доступу;
- запис власника;
- запис рівня доступу;
- запис списку доступу;
- запис списку аудиту.

Під час створення документів виконується нижченаведене правило.

Рівень доступу документа повинен бути не нижчим за мінімальний рівень доступу бази документів, в якій він міститься, та не вищим за максимальний рівень доступу цієї бази.

Додатково, для того щоб не втратити можливість доступу до документа у випадку відсутності власника, встановлюється ще одне правило, яке діє незалежно від списку доступу документа.

Користувачі з роллю *Адміністратор безпеки* отримують такі види доступу до всіх документів:

- читання атрибутів доступу;
- запис власника.

4.3.2.2 ПРД для баз із адміністративним керуванням доступом

В адміністративних базах працювати з документами можуть звичайні користувачі та адміністратори документів. Можливість доступу визначається списком доступу документа, його рівнем доступу, а також роллю та рівнем доступу користувача. Адміністратор документів, який є власником бази, завжди має право керувати доступом до документа (незалежно від списку доступу документа). Крім того, в адміністративних базах діють деякі додаткові обмеження, зокрема, керувати доступом до документів можуть лише адміністратори документів.

Користувач отримує доступ до документа, якщо виконуються наведені нижче умови.

- рівень доступу користувача не нижчий за рівень доступу документа.
- йому встановлена роль *Звичайний користувач* або йому встановлена роль *Адміністратор документів* і не встановлені ролі *Адміністратор безпеки* та *Системний адміністратор*;
- у списку доступу документа користувачу або групі, до якої він належить, не заборонено цей доступ;
- у списку доступу документа користувачу або групі, до якої він належить, надано цей доступ.

Власник бази має особливі повноваження щодо доступу до документів, які містяться в «його» базі, які діють незалежно від списку доступу документа.

Власник бази має особливі повноваження щодо доступу до документів, які містяться в «його» базі, які діють незалежно від списку доступу документа.

Якщо користувач є власником бази і йому встановлена роль *Адміністратор документів*, він отримує до документа такі види доступу:

- читання атрибутів доступу;

– запис власника;
– запис рівня доступу;
– запис списку доступу;
– запис списку аудиту.

Крім цього, для адміністративних баз встановлюються обмеження, які не дозволяють звичайним користувачам керувати доступом до документів. Ці обмеження діють незалежно від списку доступу бази.

Звичайні користувачі не можуть отримати такі види доступу до документів:
– читання атрибутів доступу;
– запис власника;
– запис рівня доступу;
– запис списку доступу;
– запис списку аудиту.

Це правило має один виняток: під час створення документа його рівень доступу визначає користувач, який створює документ.

Під час створення документів виконується нижченаведене правило.

Рівень доступу документа повинен бути не нижчим за мінімальний рівень доступу бази документів, в якій він міститься, та не вищим за максимальний рівень доступу цієї бази.

Якщо параметр політики документів (п. 4.2.2.5) *Обмеження для адміністратора документів* має значення *Так*, користувачі, яким встановлена роль *Адміністратор документів*, не можуть отримати такі види доступу (всі види доступу, крім читання та керування доступом):
– запис вмісту документа;
– запис стандартних та додаткових атрибутів;
– видалення;
– друк;
– експорт.

Користувачі, яким встановлена роль *Адміністратор документів* та роль *Адміністратор безпеки* або *Системний адміністратор*, не можуть отримати такі види доступу (всі види доступу, крім читання та керування доступом):
– запис вмісту документа;
– запис стандартних та додаткових атрибутів;
– видалення;
– друк;
– експорт.

4.3.2.3 Додаткові правила здійснення друку та експорту документів

Для виконання вимог до експорту та друку документів у системі діють такі правила, які стосуються баз із будь-яким принципом керування доступом.

Якщо рівень доступу документа не нижчий за значення параметра *мінімальний рівень доступу для використання пароля на експорт документів*, користувач отримує доступ на експорт документа лише за умови введення паролю.

Якщо рівень доступу документа не нижчий за значення параметра *мінімальний рівень доступу для використання пароля на друк документів*, користувач отримує доступ на друк лише за умови введення паролю.

Необхідність введення паролю забезпечує присутність під час друку чи експорту уповноваженої особи.

Для зберігання паролів використовуються параметри *пароль на експорт документів* та *пароль на друк документів* відповідно. Зберігається подвійне хеш-перетворення пароля.

4.3.3 Доступ до захищених папок

4.3.3.1 Загальні правила

Користувач отримує доступ до захищеної папки, якщо виконуються такі умови:

– рівень доступу користувача не нижчий за рівень доступу захищеної папки;

– у списку доступу захищеної папки користувачу або групі, до якої він належить, не заборонено цей доступ;

– у списку доступу захищеної папки користувачу або групі, до якої він належить, надано цей доступ.

Якщо для захищеної папки встановлений список процесів, користувач отримує доступ тільки у тому випадку, коли доступ здійснюється за допомогою одного з процесів, зазначених у списку.

Порядок перевірки виконання вищезазначених правил наведений у блок-схемі в розділі Д.5 додатка Д.

Наведені правила розповсюджуються на всі папки та файли, які знаходяться в захищеній папці.

4.3.3.2 Доступ до програмних засобів та даних системи ЛОЗА-2

Доступ до файлів, які відповідають програмним засобам системи ЛОЗА-2, а також до файлів, в яких зберігаються дані системи, повинен регулюватись таким же чином, що й доступ до захищених папок. Списки доступу та списки процесів відповідних папок та файлів повинні бути сталими і узгодженими з розподілом функцій між модулями системи та технологією роботи користувачів у системі.

4.3.4 Доступ до знімних дисків

Можливість доступу користувача до зареєстрованого диска USB Flash визначається списком доступу диска, його рівнем доступу та рівнем доступу користувача. Можливість доступу до дисків USB Flash, які не були зареєстровані, а також до гнучких дисків та CD/DVD-дисків визначається відповідною політикою знімних дисків (див. п. 4.2.5.1).

Користувач отримує доступ до зареєстрованого диска USB Flash, якщо виконуються такі умови:

– рівень доступу користувача не нижчий за рівень доступу диска;

– у списку доступу диска користувачу або групі, до якої він належить, не заборонено цей доступ;

– у списку доступу диска користувачу або групі, до якої він належить, надано цей доступ.

Якщо для зареєстрованого диска USB Flash встановлений список процесів, користувач отримує доступ тільки у тому випадку, коли доступ здійснюється за допомогою одного з процесів, зазначених у списку.

Користувач отримує доступ до диска USB Flash, який не був зареєстрований, до гнучкого диска або до CD/DVD-диска, якщо виконуються такі умови:

– у списку доступу відповідної політики користувачу або групі, до якої він належить, не заборонено цей доступ;

– у списку доступу відповідної політики користувачу або групі, до якої він належить, надано цей доступ.

Наведені правила регламентують доступ до всіх папок та файлів, які знаходяться на знімному диску.

4.3.5 Доступ до захищених процесів

4.3.5.1 Загальні правила

Користувач отримує доступ до захищеного процесу, якщо виконуються такі умови:

– у списку доступу процесу користувачу або групі, до якої він належить, не заборонено цей доступ;

– у списку доступу процесу користувачу або групі, до якої він належить, надано цей доступ.

4.3.5.2 Доступ до процесів системи ЛОЗА-2

Процеси, які використовуються для доступу до баз документів, документів та об’єктів, що містять технологічну інформацію, автоматично включаються до списку захищених процесів. Вони мають сталі списки доступу, наведені в таблиці 4.16. В таблиці використані такі позначення:

– «+» – користувач може отримати доступ до процесу;

– «–» – користувач не може отримати доступу до процесу.

Таблиця 4.16 – Матриця доступу до процесів

Процес / Роль користувача	Захищені документи	Керування захистом	Монітор захисту	Аудитор	Реєстрація	Інші (допоміжні) процеси
Звичайний користувач	+	–	–	–	+	+
Адміністратор безпеки	+	+	+	+	+	+
Системний адміністратор	–	+	+	–	+	+
Адміністратор документів	+	–	–	–	+	+

4.3.6 Доступ до технологічної інформації

Права на читання та запис даних до бази облікових записів, права на читання та запис даних про об'єкти захисту, права на читання та запис переліку робочих станцій та право на перегляд журналу реєстрації повинен мати лише користувач з роллю *Адміністратор безпеки*.

Права на читання та зміну значень параметрів конфігурації системи, читання оперативних даних про роботу системи та оперативне керування системою розподіляються між ролями *Адміністратор безпеки* та *Системний адміністратор*.

Можливість читати та змінювати значення параметрів конфігурації, які безпосередньо пов'язані з керуванням доступом, повинен мати лише користувач із роллю *Адміністратор безпеки*.

Для забезпечення можливості керування доступом до об'єктів, що містять технологічну інформацію, використовується параметр конфігурації ***дозволи на доступ до технологічної інформації***. Цей параметр визначає дозволи та заборони дозволу на читання та запис до кожної зі складових технологічної інформації, наведених у п. 4.2.7. Для параметрів конфігурації дозволи надаються для груп параметрів. Значення за умовчанням для цього параметра наведене в таблиці А.3 Додатка А. Частина дозволів не може бути змінена (відповідні значення виділені в таблиці сірою заливкою). Зокрема, дозволи на доступ до технологічної інформації може змінювати лише адміністратор безпеки.

Право на запис до журналу реєстрації не надається жодній ролі, оскільки реєстрацію подій у цьому журналі здійснює ядро системи.

4.4 Додаткові засоби захисту

4.4.1 Захист документів

4.4.1.1 Небезпечні команди Microsoft Excel та Microsoft Word

Деякі можливості, які надають програми Microsoft Excel та Microsoft Word під час роботи з документами, можуть призвести до порушення безпеки інформації. Це, наприклад, можливість збереження документа у файлі, можливість створення та запуску власних макросів та ін. Внутрішні команди, які відповідають таким можливостям, називатимемо *небезпечними командами*. Під час роботи з документами за допомогою програми *Захищені документи* небезпечні команди унеможливлюються.

Переліки небезпечних команд визначаються двома параметрами конфігурації, *перелік небезпечних команд Excel та перелік небезпечних команд Word*. Значення за умовчанням для цих параметрів наведені в таблицях А.4, А.5 Додатка А. Адміністратор може змінювати переліки – додавати та видаляти команди. Команди, які встановлюються за умовчанням, не можуть бути видалені.

4.4.1.2 Дозволені шаблони та надбудови

Для роботи із програмами Microsoft Excel та Microsoft Word часто використовуються шаблони, які можуть містити небезпечні, з точки зору захисту, макроси. Таку ж небезпеку можуть складати процедури, що містяться в так званих надбудовах (Addins та COM Addins). Для того, щоб надати користувачам можливість

використовувати необхідні їм шаблони та надбудови, використовуються такі параметри конфігурації:

- *перелік дозволених надбудов COM для Excel;*
- *перелік дозволених надбудов COM для Word;*
- *перелік дозволених шаблонів та надбудов Excel;*
- *перелік дозволених шаблонів та надбудов Word.*

Разом із кожним шаблоном або надбудовою зберігається контрольна сума відповідного файлу (для надбудов COM це файл бібліотеки, яка містить реалізацію відповідного класу).

Якщо шаблон або надбудова зазначені в одному з цих параметрів і відповідна контрольна сума не змінилась, вони вважаються безпечними і їх використання дозволяється. Усі інші шаблони та надбудови під час роботи користувача з документами в системі ЛОЗА-2 відключаються.

4.4.1.3 Заборонені програми

Для того, щоб змусити користувачів працювати з текстовими документами та електронними таблицями тільки за допомогою програми *Захищені документи*, використовується заборона запуску програм. Заборонені програми не можуть бути запущені на комп'ютері.

Для того, щоб вказати, які саме програми є забороненими, використовуються два параметри конфігурації:

- *фіксовані заборонені програми;*
- *додаткові заборонені програми.*

За допомогою першого параметра можна заборонити виконання чотирьох стандартних програм: Microsoft Word, Microsoft Excel, Microsoft WordPad та Microsoft Блокнот.

Другий параметр дозволяє заборонити виконання будь-яких інших програм. Він містить перелік файлів, що відповідають забороненим програмам.

4.4.1.4 Диски для зберігання документів

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

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

Ці 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*. Користувачі системи не мають безпосереднього доступу до цієї папки і отримують доступ до баз документів та документів тільки за допомогою програмних засобів для роботи з документами із складу системи ЛОЗА-2.

Наведені параметри визначаються окремо для сервера та кожної робочої станції. Диски, визначені для сервера, можуть бути надані у спільне користування. Для цього використовуються такі параметри конфігурації:

- *спільні гнучкі диски для зберігання документів*
- *спільні жорсткі диски для зберігання документів;*

– *спільні знімні диски для зберігання документів;*
– *спільні компакт-диски для зберігання документів.*

Доступ до баз документів, які знаходяться на дисках, наданих у спільне користування, можуть отримати всі користувачі мережі.

4.4.2 Забезпечення безпеки середовища

Для забезпечення обмежень на роботу користувачів, перелічених у п. 4.1.5, система ЛОЗА-2 відстежує виконання перелічених нижче вимог.

1) Має бути встановлена вимога натискання комбінації клавіш Ctrl+Alt+Del під час входу до системи.

2) Має бути встановлений контроль входу до ОС засобами системи ЛОЗА-2.

3) В ОС Windows XP/2003 має бути відключена можливість запускати прикладні програми від імені іншого користувача. В ОС Windows Vista/7/8/8.1/10/2008/2012 вказана можливість зберігається.

4) ОС Windows XP/Vista/7/8/8.1/10/2008/2012 дозволяють перевести комп'ютер у режими сну (hibernate) та очікування (suspend). Система ЛОЗА-2 забороняє використання цих режимів, оскільки під час виходу з режиму сну автентифікація користувача взагалі не виконується, а під час виходу зі стану очікування автентифікація проводиться лише у випадку встановлення додаткового параметра, який адміністратор може не встановити.

5) Служба *LOZAStarter* має бути налаштована на автоматичний запуск.

6) Під час перебування системи в робочому стані має бути запущений драйвер *LOZAFilt*.

7) В ОС Windows Vista/7/8/8.1/10/2008/2012 має бути відключений інструмент *Ножиці*.

Всі налаштування ОС, які відповідають зазначеним вимогам, встановлюються під час інсталяції системи ЛОЗА-2.

Перевірка цих налаштувань виконується так само, як і перевірка цілісності: постійно під час перебування системи в робочому стані, на початку роботи та під час виходу зі стану відновлення. Виконання перевірки складає зміст операції *Перевірка безпеки середовища*.

Якщо порушення безпеки середовища виявляється під час перебування системи в робочому стані, виконується аварійне завершення роботи.

Якщо ж порушення виявляється під час виходу зі стану відновлення або на початку роботи, система повідомляє про відповідну помилку. Якщо адміністратор обирає для обробки помилки опцію *Ігнорувати* (див. п. 3.6), відповідні налаштування Windows відновлюються і виконується перезавантаження Windows.

4.4.3 Безпечне видалення файлів

Для безпечного видалення файлів застосовується процедура безповоротного видалення (wipe), яка виключає можливість відновлення.

4.4.3.1 Видалення об'єктів захисту

Система ЛОЗА-2 забезпечує безпечне (без можливості відновлення) видалення файлів, в яких зберігаються такі об'єкти захисту:

– бази документів;
– документи;
– папки та файли, які знаходяться у захищених папках;
– папки та файли. які знаходяться на зареєстрованих знімних дисках;

– папки та файли, які знаходяться на знімних дисках, до яких застосовуються політики знімних дисків;
– технологічна інформація.

4.4.3.2 Видалення тимчасових файлів

В системі ЛОЗА-2 передбачена можливість автоматичного видалення тимчасових файлів. Для цього передбачені три параметри конфігурації:
– *видаляти тимчасові файли користувачів;*
– *перелік тимчасових папок;*
– *перелік тимчасових файлів.*

Перший параметр може приймати значення *Так* або *Ні.* Він визначає, чи виконується автоматичне видалення папок та файлів, які містяться в тимчасових папках користувачів. Кожний користувач може мати дві тимчасові папки, на які вказують змінні оточення *Temp* та *Tmp*. Звичайно, обидві вони вказують на папку *%USERPROFILE%\Local Settings\Temp*.

Параметр *перелік тимчасових папок* містить перелік папок, які вважаються тимчасовими. Усі папки та файли, які містяться в цих папках, видаляються.

Параметр *перелік тимчасових файлів* містить перелік імен файлів, які вважаються тимчасовими. Кожне ім'я може бути шаблоном, тобто містити символи «?» та «*». Усі файли, які містяться в переліку або відповідають хоча б одному із шаблонів, що міститься в переліку, видаляються.

Видалення тимчасових файлів користувачів, файлів, які містяться в тимчасових папках, та тимчасових файлів відбувається на початку роботи системи, під час завершення роботи системи, під час входу користувачів до системи та під час виходу користувачів із системи.

4.4.4 Заборона 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 (див. п. 4.2.3.1);
– встановлення аудиту друку документа, що забезпечує докладну реєстрацію подій друку (див. п. 4.2.3.1);
– встановлення пароля на друк (див. п. 4.3.2.3).

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 усім);*
– *усім (друк заборонений усім);*
– *усім користувачам системи ЛОЗА-2, крім адміністраторів безпеки;*

– *усім користувачам системи ЛОЗА-2, крім адміністраторів документів;*

– *усім користувачам системи ЛОЗА-2, 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.

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 встановити 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 із 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*).

5 Перевірка цілісності програмного середовища

Перевірки цілісності програмного середовища на сервері здійснює *Сервер безпеки*, перевірки на робочій станції виконує *LOZAGuard*.

Перевірки виконуються автоматично, але в разі необхідності адміністратор може ініціювати будь-яку перевірку за допомогою програми *Монітор захисту*.

5.1 Загальні правила перевірки

Параметр конфігурації *об'єкти для перевірки цілісності* визначає що саме підлягає перевірці, а також дозволяє встановити режим перевірки.

Може бути перевірена цілісність таких об'єктів:

- файли та папки;
- розділи та параметри системного реєстру;
- завантажувальні сектори жорстких дисків комп'ютера;
- облікові записи.

Для кожного виду об'єктів встановлюється режим перевірки. Перевірки можуть виконуватись:

- при старті;
- періодично;
- постійно (тільки файли та папки і розділи та параметри реєстру).

Перевірка при старті є обов'язковою, якщо встановлена періодична або постійна перевірка.

Періодична перевірка означає проведення перевірок з інтервалом, який визначається параметром конфігурації *періодичність перевірок цілісності* (він задає час у хвилинах).

Постійна перевірка – це перевірка "у реальному часі", система реагує на зміни одразу після їх виникнення. Для проведення постійної перевірки використовуються засоби нотифікації Windows, тому вона не виявляє змін, що виникли після використання безпосереднього доступу до жорсткого диска (наприклад, за допомогою програми *DiskProbe*). Якщо існує загроза виникнення таких змін, для всіх видів об'єктів слід встановити періодичну перевірку цілісності. У протилежному випадку періодично перевіряти цілісність файлів та папок і розділів та параметрів реєстру не має потреби – для забезпечення цілісності досить постійної перевірки.

Якщо параметр *об'єкти для перевірки цілісності* визначає перевірку завантажувальних секторів, перевіряються всі завантажувальні сектори фізичних та логічних дисків.

Для файлової системи, реєстру та облікових записів перелік об'єктів, що перевіряються, визначається додатковими параметрами, які описані нижче, у п. 5.2, 5.3 та 5.5. Разом із файлами, папками та розділами реєстру перевіряється цілісність їхніх дескрипторів безпеки (для файлів та папок – у тому випадку, коли вони знаходяться на томах NTFS).

Для кожного виду об'єктів перевірки формується і запам'ятовується відповідний "відбиток". Під час перевірки такий же "відбиток" формується знову і порівнюється з попереднім. У результаті порівняння система робить висновок про наявність змін, а відтак і порушень цілісності.

Для формування відбитка всіх об'єктів, крім завантажувальних секторів, використовуються контрольні суми (п. 5.6). Завантажувальні сектори запам'ятовуються безпосередньо.

Окрім виявлення змін під час перевірки можливе виникнення ситуацій, які заважають її проведенню. За ступенем важливості вони поділяються на помилки та попередження.

Помилки – це ситуації, які повністю або частково унеможливлюють перевірку (наприклад, відмова в доступі до файлу, який перевіряється). У разі виявлення помилки цілісність вважається порушеною.

Попередження виникають у тому випадку, коли виявляється некоректність параметрів перевірки (наприклад, одна із зазначених для перевірки папок міститься в іншій). Такі ситуації не перешкоджають проведенню перевірки і не вважаються порушеннями цілісності.

Перевірки цілісності здійснюються під час перебування системи в робочому стані.

У разі виявлення порушення цілісності система здійснює аварійне завершення роботи (п. 3.4) або переходить у стан відновлення – в залежності від значення параметра конфігурації *реакція на порушення цілісності*. Якщо здійснюється аварійне завершення роботи, на початку наступного сеансу система потрапляє в стан відновлення.

У стані відновлення постійні та періодичні перевірки не проводяться.

Під час виходу зі стану відновлення для всіх видів об'єктів, для яких зазначена перевірка при старті, знову проводиться перевірка цілісності. Вихід із стану здійснюється лише в тому випадку, коли перевірка не виявляє змін (це означає, що відновлення було проведене успішно). У випадку виявлення змін програмного середовища система залишається в стані відновлення.

Звіт про кожну перевірку, який містить відомості про всі знайдені та прийняті зміни, помилки та попередження, зберігається у файлі. Для кожної групи об'єктів, що перевіряються, може бути заданий окремий файл звіту (але не забороняється зазначити для всіх звітів один файл). Імена файлів визначаються такими параметрами конфігурації:

– *ім'я файлу звіту про перевірку цілісності файлів та папок;*

– *ім'я файлу звіту про перевірку цілісності розділів та параметрів реєстру;*

– *ім'я файлу звіту про перевірку цілісності завантажувальних секторів;*

– *ім'я файлу звіту про перевірку цілісності облікових записів.*

Для кожного з файлів може бути заданий граничний розмір, для цього використовуються такі параметри:

– *граничний розмір файлу звіту про перевірку цілісності файлів та папок;*

– *граничний розмір файлу звіту про перевірку цілісності розділів та параметрів реєстру;*

– *граничний розмір файлу звіту про перевірку цілісності завантажувальних секторів;*

– *граничний розмір файлу звіту про перевірку цілісності облікових записів.*

У разі перевищення граничного розміру старі записи видаляються з файлу.

Відомості про останню проведену перевірку можна переглянути за допомогою програми *Монітор захисту*. Під час перебування системи в стані відновлення ця

програма дозволяє також провести перевірку та прийняти зміни в складі програмного середовища.

5.2 Перевірка файлів та папок

5.2.1 Параметри перевірки

Перелік файлів та папок, які перевіряються, визначається такими параметрами конфігурації:

– *перелік типів файлів для перевірки цілісності;*

– *перелік папок для перевірки цілісності;*

– *перелік папок, для яких не здійснюється перевірка цілісності;*

– *перелік файлів для перевірки цілісності;*

– *перелік файлів, для яких не здійснюється перевірка цілісності.*

Тип файлу визначається за його розширенням. Перевірці підлягають усі папки та файли, які визначаються першими двома переліками (усі зазначені папки та всі файли зазначених типів, які знаходяться в зазначених папках), та, додатково, усі файли, вказані в четвертому переліку. Папки, вказані в третьому переліку, та файли, вказані в останньому переліку, не перевіряються.

Для кожної папки із другого переліку можна зазначити, що перевірка стосується вкладених папок, – у протилежному випадку перевірятимуться лише такі об'єкти:

– сама папка – на видалення та зміни дескриптора безпеки;

– файли, що в ній знаходяться, – на зміни, видалення, створення та зміни дескрипторів безпеки;

– вкладені папки першого рівня (без файлів, які в них знаходяться) – на видалення, створення та зміни дескрипторів безпеки.

В усіх переліках файлів та папок дозволяється використання змінної оточення Windows, а також рядка %*LOZA*%, який позначає кореневу папку системи ЛОЗА-2.

Параметр *перелік типів файлів для перевірки цілісності* слід встановити таким чином, щоб перевірялись всі файли, які можна вважати файлами, що виконуються, – безпосередньо (як, наприклад, файли **.exe* та **.dll* або файли сценаріїв **.cmd*) або опосередковано (як, наприклад, файли драйверів **.drv* або файли шаблонів MS Word **.dot*).

Для того, щоб забезпечити перевірку цілісності всіх програмних засобів системи ЛОЗА-2, для параметрів *перелік типів файлів для перевірки цілісності, перелік папок для перевірки цілісності та перелік файлів для перевірки цілісності* визначені обов'язкові елементи (їх не можна видалити під час коригування значень відповідних параметрів). Відповідні відомості наведені в таблиці А.1 у Додатку А.

5.2.2 Характеристики, які перевіряються

Під час формування "відбитка" запам'ятовується перелік папок із їхніми дескрипторами безпеки (для томів NTFS) та перелік файлів із їхніми дескрипторами безпеки (для томів NTFS) і контрольними сумами (п. 5.6).

У результаті перевірки можуть бути виявлені такі порушення цілісності:

– змінені файли;

– нові файли;
– видалені файли;
– змінені дескриптори безпеки файлів;
– нові папки;
– видалені папки;
– змінені дескриптори безпеки папок.

5.3 Перевірка розділів та параметрів реєстру

5.3.1 Параметри перевірки

Перелік розділів та параметрів реєстру, які перевіряються, визначається такими параметрами конфігурації системи:

– *перелік розділів реєстру для перевірки цілісності;*
– *перелік розділів реєстру, для яких не здійснюється перевірка цілісності;*
– *перелік параметрів реєстру для перевірки цілісності;*
– *перелік параметрів реєстру, для яких не здійснюється перевірка цілісності.*

Перевірці підлягають усі розділи та параметри, які визначаються першим переліком (усі зазначені розділи та всі параметри, які знаходяться в зазначених розділах), та, додатково, усі параметри, вказані в третьому переліку. Розділи, вказані в другому переліку, та параметри, вказані в четвертому переліку, не перевіряються.

Для кожного розділу з першого переліку можна зазначити, що перевірка стосується вкладених підрозділів, – у протилежному випадку перевірятимуться лише такі об’єкти:

– сам розділ – на видалення та зміни дескриптора безпеки;
– параметри, що в ньому знаходяться – на зміни, видалення та створення;
– вкладені розділи першого рівня – на видалення, створення та зміни дескрипторів безпеки.

Для того, щоб забезпечити перевірку цілісності розділів реєстру, у яких зберігаються параметри конфігурації системи, до параметра *перелік розділів реєстру для перевірки цілісності* обов’язково включається розділ *HKEY_LOCAL_MACHINE\SOFTWARE\NIIavtoprom\LOZA-2* і визначається перевірка вкладених у нього розділів (див. таблицю А.1 у Додатку А). Видалити цей розділ із переліку неможливо.

5.3.2 Характеристики, які перевіряються

Під час формування “відбитка” запам’ятовується перелік розділів із їхніми дескрипторами безпеки та перелік параметрів із їхніми контрольними сумами (див. п. 5.6).

У результаті перевірки можуть бути виявлені такі порушення цілісності:

– змінені параметри;
– нові параметри;
– видалені параметри;
– нові розділи;
– видалені розділи;
– змінені дескриптори безпеки розділів.

5.4 Перевірка завантажувальних секторів

Перевіряються завантажувальні сектори всіх фізичних та логічних дисків. Для подальших порівнянь запам'ятовується не контрольна сума сектора, а весь сектор безпосередньо (це не викликає надмірних витрат дискового простору, оскільки один завантажувальний сектор займає 512 байтів).

У результаті перевірки можуть бути виявлені такі порушення цілісності:

- змінені сектори;
- нові сектори;
- видалені сектори.

5.5 Перевірка облікових записів

5.5.1 Параметри перевірки

Перевіряються всі облікові записи, які містяться в базі облікових записів ОС, за винятком тих, які зазначені в параметрі конфігурації *перелік облікових записів, для яких не здійснюється перевірка цілісності*.

5.5.2 Характеристики, які перевіряються

Під час формування "відбитка" запам'ятовується перелік облікових записів локальних груп та користувачів. Для кожної групи запам'ятовуються її члени, для кожного користувача – інтегральна контрольна сума (див. п. 5.6) усіх його властивостей: імені, повного імені, сценарію входу, домашньої папки та ін.

У результаті перевірки можуть бути виявлені такі порушення цілісності:

- нові групи;
- видалені групи;
- нові члени груп;
- видалені члени груп;
- змінені користувачі;
- нові користувачі;
- видалені користувачі.

5.6 Обчислення контрольних сум

Для відстеження змін об'єктів (файлів, параметрів реєстру та облікових записів) використовуються їхні контрольні суми – спеціальні числа, які з високою ймовірністю є унікальними для вмісту об'єкта.

Контрольні суми підраховуються за допомогою поширеного методу, який називається циклічним контролем за надлишком (CRC – *Cyclic Redundancy Check*). Він забезпечує виявлення змін з імовірністю $1\text{-}2^{-n}$, де n позначає розрядність контрольної суми. Для підрахунку обрано $n = 32$, тому відповідна ймовірність дорівнює приблизно 0,99999999976.

Як дільник обрано 33-розрядне шістнадцяткове число 104C11DB7 (воно є стандартним для протоколів *EtherNet*, а також використовується поширеним архіватором *WinZIP*). Для прискорення процесу обчислення контрольних сум використовується табличний метод.

6 Реєстрація подій

Під час роботи системи відбувається реєстрація різноманітних подій. Ці події поділяються на дві групи:

- події, пов’язані з роботою системи;
- події, пов’язані з реєстрацією дій користувачів.

Повний перелік подій, які реєструє система ЛОЗА-2, наведений у Додатку Б.

6.1.1 Реєстрація подій, пов’язаних із роботою системи

Ядро системи реєструє всі важливі події, які пов’язані з її функціонуванням. Це такі події, як початок роботи та завершення роботи системи, виявлення порушень цілісності, прийняття змін у складі програмного середовища тощо. Вони можуть мати тип *Інформація*, *Попередження* або *Помилка*.

Для реєстрації цих подій (згідно із загальноприйнятими в Windows правилами) використовується журнал прикладних програм (*Журнал приложений*, *Application Log*).

Події реєструються від імені джерела *LOZASystem*. Вони розподілені на категорії, наведені в таблиці 6.1.

Таблиця 6.1 – Категорії подій

Назва	Пояснення
Робота системи	Початок та завершення роботи системи, зміна стану системи та ін.
Цілісність	Виявлення порушень цілісності, прийняття змін та ін.
Робочі станції	Читання та коригування переліку робочих станцій

6.1.2 Реєстрація дій користувачів

Для реєстрації дій користувачів використовується *журнал реєстрації* (див. п. 6.1.3). Відповідні події мають тип *Аудит успіхів* або *Аудит відмов* і реєструються від імені джерела *LOZAAudit*. У разі, коли користувач отримує дозвіл на виконання дії, реєструється подія, яка має тип *Аудит успіхів*, у протилежному випадку – подія, яка має тип *Аудит відмов*. Події джерела *LOZAAudit* розподілені на категорії, наведені в таблиці 6.2.

Таблиця 6.2 – Категорії подій

Назва	Пояснення
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
Облікові записи	Коригування бази облікових записів та даних про об’єкти 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	Читання бази, створення документів, коригування бази та ін.
Керування об'єктами	Створення, коригування атрибутів і видалення захищених папок, зареєстрованих змінних носіїв та захищених процесів
Доступ до об’єктів	Читання та запис папок і файлів, які знаходяться у захищеній папці, на змінному диску, а також запуск захищеного процесу

У тому випадку, коли внаслідок збою реєстрація подій у журналі реєстрації неможлива, події реєструються в журналі прикладних програм Windows від імені джерела *LOZAAudit* (після полагодження журналу реєстрації всі вони будуть імпортовані до нього).

6.1.3 Журнали реєстрації

Журнал реєстрації призначений для того, щоб зібрати в одному переліку всі події, пов’язані з безпекою інформації. Цей журнал формується засобами системи ЛОЗА-2 із подій, зареєстрованих у журналах Windows (у тому числі подій, які були зареєстровані в журналі прикладних програм від імені джерела *LOZASystem*), а також за рахунок безпосередньої реєстрації подій аудиту (п. 6.1.7).

В системі LOZA-2 розрізняються журнал реєстрації подій сервера та журнали реєстрації подій робочих станції.

Журнал реєстрації подій сервера поєднує події, які відбуваються на сервері, та деякі події, які відбуваються на робочих станціях.

Під час роботи системи відбувається аналіз подій, які з’являються в журналах Windows, і частина подій імпортується до журналу реєстрації подій сервера та робочих станцій, що надає можливість перегляду відібраних подій та формування довільних протоколів роботи. Те, які саме події імпортуються, визначається трьома параметрами конфігурації:

- *перелік подій, які імпортуються до журналу;*
- *копіювання подій до журналу сервера;*
- *імпортувати всі помилки.*

Перший параметр дозволяє для кожного журналу Windows встановити перелік подій, які необхідно імпортувати. Рекомендоване значення для цього параметра (воно встановлюється за умовчанням) наведене в Додатку А.

Другий параметр дозволяє для кожного журналу реєстрації подій робочої станції встановити перелік подій, які необхідно копіювати до журналу реєстрації подій сервера. Рекомендоване значення для цього параметра (воно встановлюється за умовчанням) наведене в таблиці А.7 додатку А.

Якщо третій параметр має значення *Так*, усі події з журналів Windows, які мають тип *Помилка*, імпортуються до журналу реєстрації (незалежно від того, чи зазначені вони в першому параметрі).

Імпорт подій відбувається постійно під час роботи системи. На початку роботи система переглядає журнали Windows і за необхідності імпортує до журналу події, які з'явились після останнього завершення її роботи.

Журнал реєстрації сервера зберігається у файлі *%LOZA%\Security\Log\SecLog\seclog.lzl* на сервері. Журнал реєстрації робочої станції зберігається у файлі *%LOZA%\Security\Log\SecLog\seclog.lzl* на робочій станції. Граничний розмір цих файлів визначається параметром конфігурації *граничний розмір журналу* для кожного журналу окремо. Після досягнення граничного значення нові події записуються замість старих.

Для збереження зареєстрованих раніше подій здійснюється резервне копіювання журналу. Резервні копії журналу реєстрації сервера зберігаються в папці *%LOZA%\Security\Log\Backup* на сервері. Резервні копії журналу реєстрації робочої станції зберігаються в папці *%LOZA%\Security\Log\Backup* на робочій станції та в папці *%LOZA%\Security\Log\Backup\Workstations\<ім'я робочої станції>* на сервері. Файли копій мають імена *Lg<ddmmyy>_<nn…n>.lzl*, де *ddmmyy* позначає дату створення копії (день, місяць та останні дві цифри року), а *nn…n* – номер копії журналу, створеної у певний день. Остання резервна копія знаходиться у файлі *Last.lzl*. Усі події, які реєструються в журналі реєстрації, одночасно дублюються в цьому файлі. Адміністратор може налаштувати систему таким чином, що старі резервні копії журналу реєстрації будуть поступово видалятись (п. 6.1.5).

Для роботи з журналом реєстрації та з його резервними копіями призначена програма *Аудитор*. Вона дозволяє переглядати журнал, надає зручні засоби для пошуку подій, дозволяє формувати звіт про небезпечні події, створювати протоколи роботи системи, а також працювати з копіями журналу та зберігати журнал у вигляді файлу.

6.1.4 Небезпечні події

6.1.4.1 Перелік небезпечних подій

Деякі з подій, що фіксуються в журналі реєстрації, свідчать про можливе порушення безпеки інформації. Такі події називаються *небезпечними*, перелік цих подій визначається двома параметрами конфігурації:

- *перелік небезпечних подій;*
- *вважати помилки небезпечними подіями*.

Перший параметр дозволяє для кожного джерела подій кожного журналу Windows встановити перелік подій, які слід вважати небезпечними.

Якщо другий параметр має значення *Так*, усі події, зареєстровані в журналі під час роботи системи, які мають тип *Помилка*, вважаються небезпечними (незалежно від того, чи зазначені вони в першому параметрі).

Небезпечними можуть бути лише ті події, які були імпортовані до журналу. Тому події, зазначені в параметрі *перелік небезпечних подій*, але не зазначені в параметрі *перелік подій, які імпортуються до журналу*, небезпечними не вважатимуться. Крім того, події джерела *LOZAAudit*, які не імпортуються, а реєструються в журналі реєстрації безпосередньо, не можуть вважатися небезпечними.

Рекомендоване значення для параметра *перелік небезпечних подій* (воно встановлюється за умовчанням) наведене в Додатку В. Слід звернути увагу на те, що в деяких випадках зазначені події реєструються внаслідок цілком безпечних дій – відповідні пояснення також наведені в Додатку В.

Для того, щоб вважати небезпечними цілком “безпечні” події, діє один виняток: подія *#560* (“Доступ до об’єктів”, журнал безпеки, джерело *Security*) вважається небезпечною лише в тому випадку, коли в її описі містяться рядки “*WRITE_OWNER*”, “*WRITE_DAC*” або “*ACCESS_SYS_SEC*” – це означає коригування атрибутів доступу об’єкта, відповідно його власника, списку доступу та списку аудиту.

6.1.4.2 Реакція на небезпечні події

У системі передбачені такі способи реагування на небезпечні події:
- створення звіту про небезпечні події;
- звукова сигналізація;
- зміна стану системи (серверної чи клієнтської частини);
- видача повідомлення на консоль адміністратора;
- виконання командного файлу.

Система реагує лише на ті небезпечні події, які реєструються в журналі під час роботи системи. Небезпечні події, імпортовані під час перегляду журналів Windows на початку роботи системи (п. 6.1.3), не викликають реакції.

6.1.4.2.1 Звіт про небезпечні події

Одразу після реєстрації у журналі реєстрації будь-якої із зазначених подій автоматично створюється *Звіт про небезпечні події*. У залежності від значення параметра конфігурації *створення звіту про небезпечні події* звіт може бути надрукований та/або збережений у файлі.

Файли звітів зберігаються на сервері у форматі RTF у папці *%LOZA%\Security\Log\Report* і мають імена *Rp<ddmmyy>_<nn…n>.rtf*, де *ddmmyy* позначає дату створення звіту (день, місяць та дві останні цифри року), а *nn…n* – номер звіту, створеного в певний день.

Впродовж однієї доби всі звіти зберігаються у файлі з одним і тим же іменем, тобто кожний новий звіт „затирає” попередній. Це не призводить до втрати відомостей про небезпечні події, оскільки впродовж доби інформація про небезпечні події накопичується.

Форма звіту наведена в Додатку Г. Він містить кількість та ідентифікатори виявлених протягом сеансу роботи небезпечних подій. Відомості про виявлені помилки наводяться окремо.

Друк звіту або виникнення файлу звіту на диску слугує адміністратору сигналом про можливе порушення безпеки інформації.

За необхідності *Звіт про небезпечні події* можна сформувати за допомогою програми *Аудитор* (меню *Протоколи*).

6.1.4.2.2 Звукова сигналізація

Якщо параметр конфігурації *звукова сигналізація про небезпечні події* має значення *Так*, реєстрація в журналі реєстрації кожної небезпечної події супроводжується звуковим сигналом, який відповідає стандартній події Windows *Критическая ошибка*.

6.1.4.2.3 Зміна стану

Якщо параметр конфігурації *зміна стану після небезпечної події* має значення *Перехід у стан відновлення*, під час перебування системи в робочому стані одразу після реєстрації у журналі реєстрації небезпечної події система перейде у стан відновлення.

6.1.4.2.4 Видача повідомлення на консоль адміністратора

Якщо параметр конфігурації *інформувати адміністратора про небезпечні події* має значення *Так*, одразу після реєстрації у журналі небезпечної події повідомлення про це видаються на екран всіх комп'ютерів, які призначені робочими місцями адміністратора.

6.1.4.2.5 Виконання командного файлу

Якщо параметр конфігурації *виконання командного файлу* має деяке значення, одразу після реєстрації у журналі небезпечної події повідомлення про це відбувається виконання даного командного файлу.

6.1.5 Видалення старих звітів та копій журналу

Для того, щоб не захаращувати жорсткий диск копіями журналу реєстрації та звітами про небезпечні події, можна використати автоматичне видалення старих копій. Правила видалення визначаються такими параметрами конфігурації:

- *видаляти старі звіти та копії журналу;*
- *максимальний вік звітів та копій журналу;*
- *видаляти лише архівні звіти та копії журналу*.

Перший параметр визначає, чи відбувається автоматичне видалення звітів та копій журналу, другий дозволяє встановити максимальний вік файлів, які не видаляються (у днях), за допомогою третього параметра можна заборонити видалення файлів, для яких встановлений атрибут *архівний* (звичайно, цей атрибут знімають програми резервного копіювання).

6.1.6 Протоколи роботи системи

На підставі подій, зареєстрованих у журналі реєстрації, програма *Аудитор* дозволяє створити такі протоколи:

- протокол друку документів;
- протокол за вибором.

Протокол друку створюється за датою чи інтервалом дат.

У протоколі друку зазначається інформація, яка стосується події джерела *LOZAAudit*: *Спроба друку документа* (категорія *Доступ до документів*, код *58004*). Про кожну подію друку в протоколі зазначається така інформація:

- дата та час друку документа;
- ім'я користувача, що друкував документ;
- ім'я комп'ютера;
- принтер, на якому надрукований документ;
- назва документа;
- гриф обмеження доступу документа;
- обліковий номер документа;
- кількість примірників;
- кількість аркушів в одному примірнику.

Форма протоколу друку наведена в Додатку Г.

Протокол за вибором створюється за вказаними критеріями відбору (за всіма подіями, за якоюсь подією, за категорією подій, за діями певного користувача тощо).

Протоколи створюються у вигляді файлів у форматі RTF, одразу після створення викликається програма Microsoft Word для перегляду протоколу.

6.1.7 Політика аудиту системи ЛОЗА-2

Аудит – це реєстрація дій користувачів, які пов'язані з безпекою системи. У тому разі, коли користувач отримує дозвіл на виконання дії, реєструється подія, яка має тип ***Аудит успіхів***, у протилежному випадку – подія, яка має тип ***Аудит відмов***. Політика аудиту визначає, які з цих дій підлягають реєстрації.

Політика аудиту системи ЛОЗА-2 визначається однойменним параметром конфігурації (параметр ***політика аудиту***) і стосується лише подій, які належать до джерела *LOZAAudit*. Аудит встановлюється для категорій подій, наведених у п. 6.1.1:

- вхід/вихід;
- робота з програмами;
- керування доступом;
- керування системою;
- конфігурація;
- доступ до документів;
- доступ до баз документів;
- робочі станції;
- доступ до захищених папок;
- доступ до знімних дисків;
- доступ до захищених процесів.

Аудит може бути встановлений окремо для різних видів доступу, а також для успішних та невдалих спроб доступу. Для параметрів конфігурації аудит може бути встановлений для різних груп параметрів (таблиця А.2). Для подій доступу до документів аудит може бути встановлений для різних типів документа (документ Word або таблиця Excel) та рівнів доступу документа, а для подій доступу до баз документів – у залежності від максимального рівня доступу бази.

Аудит доступу до документів та баз документів додатково регулюється списками доступу документів та баз документів (пп. 4.2.2.1 та 4.2.3.1).

Значення за умовчанням для параметра ***політика аудиту*** наведене в Додатку А.

7 Засоби автоматизації

Система ЛОЗА-2 містить засоби автоматизації, які можуть бути використані, наприклад, для вирішення таких завдань:

- автоматичне виконання деяких адміністративних завдань;
- інформування адміністратора про виникнення важливих подій;
- зв’язок з іншими інформаційними системами.

Автоматизація полягає у виконанні перелічених в таблиці 7.1 команд. Кожна команда характеризується такими параметрами:

- параметр конфігурації, який визначає команду;
- події, у випадку настання яких виконується команда;
- параметри командного рядка.

Всі зазначені параметри визначаються окремо для кожного комп'ютера мережі.

Таблиця 7.1

Параметр конфігурації	Події	Параметри	Приклади
Команда для обробки резервної копії журналу	Створення резервної копії журналу	%f – ім'я файлу резервної копії	*copy %f C:\LogArchive*
Команда для сигналізації про зміну стану	Перехід системи у певний стан	%c – код стану; %n –назва стану	*ShowMessageFromService* "Система змінила стан. Новий стан – %n."
Команда для сигналізації про небезпечну подію	Виникнення небезпечної події	%c – ім’я комп’ютера; %l – ім’я журналу; %s – ім’я джерела; %e – код події	*WriteToLog* "Виникла небезпечна подія. Джерело: %s. Код: %e"
Команда для сигналізації про помилку під час виконання операції	Виникнення помилки під час виконання операції	%c – код операції; %n – назва операції; %m – повідомлення про помилку	*ShowMessageFromService* "Помилка під час виконання операції. Операція: %c. Повідомлення: %m"
Команда для сигналізації про порушення цілісності	Порушення цілісності	%c – код типу об’єктів, цілісність яких порушено. Може бути сумою таких значень: 1 – *завантажувальні сектори;* 2 – *папки та файли;* 4 – *розділи та параметри реєстру;* 8 – *облікові записи;* *4096 – середовище*	*ShowMessageFromService* "Порушення цілісності"

У випадку необхідності передачі рядка, що співпадає із позначенням параметру, використовується "екранування" за допомогою додаткового символу "%". Наприклад,

ShowMessageFromService "Помилка під час виконання операції. Операція: %c. Використаний параметр %%c"

ДОДАТОК А. Параметри конфігурації системи

У цьому додатку наведений повний перелік параметрів конфігурації системи ЛОЗА-2, а також різноманітні технічні відомості про параметри конфігурації.

Повний текст додатку міститься у файлі *LOZA-2_SecDescr_A.pdf*, який знаходиться в папці *Doc* на дистрибутивному диску системи.

ДОДАТОК Б. Події, які реєструються системою ЛОЗА-2

У цьому додатку наведений повний перелік подій, які реєструються програмними засобами системи ЛОЗА-2 у журналі реєстрації та у журналі прикладних програм Windows.

Повний текст додатку міститься у файлі *LOZA-2_SecDescr_B.pdf*, який знаходиться в папці *Doc* на дистрибутивному диску системи.

ДОДАТОК В. Перелік небезпечних подій

Під час роботи системи можуть виникати події, на які слід звернути особливу увагу, оскільки їх виникнення може свідчити про спробу (або підготовку до спроби) несанкціонованого доступу до інформації. Якщо такі події реєструються протягом дня, відповідна інформація фіксується у звіті про небезпечні події. Перелік цих подій визначається параметром конфігурації системи *перелік небезпечних подій*. За умовчанням у переліку містяться події, наведені в таблиці В.1 Усі вони реєструються в журналі *Security* Windows і мають джерело *Security*. У стовпчику *Пояснення* вказано, яким саме діям користувачів вони відповідають.

Більшість із цих подій не повинні з'являтись після інсталяції системи ЛОЗА-2 або можуть з'являтись лише у виключних випадках (наприклад, зміна політики аудиту Windows). Такі події в останньому стовпчику таблиці помічені знаком оклику. Їх виникнення потребує негайного аналізу причин їх появи і, в разі необхідності, вжиття відповідних заходів.

Інші події можуть виникати під час роботи системи в результаті звичайної роботи адміністраторів. Ці події помічені знаком питання, а в стовпчику *Пояснення* додатково вказано, в яких випадках їх виникнення є безпечним. В інших випадках поява таких подій потребує такої ж реакції, як і виникнення подій першої групи.

Таблиця В.1

Категорія	Код	Опис (українською мовою)	Пояснення	
Системное событие	516	Вичерпані внутрішні ресурси, виділені для черги повідомлень аудиту. Можлива втрата деяких результатів аудиту. Кількість відхилених повідомлень аудиту: <...>	Подія виникає в разі збою під час здійснення аудиту, що призводить до втрати частини записів аудиту	!
Системное событие	517	Очищення журналу аудиту Основний користувач: <...> Домен: <...> Код входу: <...> Користувач-клієнт: <...> Домен клієнта: <...> Код входу клієнта: <...>	Подія виникає при очищенні журналу безпеки Windows (тобто видаленні з нього всіх подій)	!
Доступ к объектам)	560	Відкриття об'єкта Сервер об'єкта: <...> Тип об'єкта: <...> Ім'я об'єкта: <...> Новий код дескриптора: <...> Код операції: <...> Код процесу: <...> Основний користувач: <...> Домен: <...> Код входу: <...> Користувач-клієнт: <...> Домен клієнта: <...> Код входу клієнта: <...> Доступ: <...> Привілеї: <...>	Подія виникає при доступі до об'єкта. За умовчанням подія вважається небезпечною, якщо опис події містить один із рядків „WRITE_OWNER", „ACCESS_SYS_SEC", „WRITE_DAC" (вони означають відповідно зміну власника об'єкта, встановлення аудиту доступу до об'єкта та зміну дозволів на доступ до об'єкта)[1]	!

Категорія	Код	Опис (українською мовою)	Пояснення	
Изменение политики	608	Присвоєння прав користувачеві Право: <...> Присвоєно: <...> Виконавець: <...> Користувач: <...> Домен: <...> Код входу: <...>	Подія виникає, якщо користувачеві або групі користувачів було присвоєне певне право	!
Изменение политики	609	Видалення прав користувача Право: <...> Видалено для: <...> Виконавець: <...> Користувач: <...> Домен: <...> Код входу: <...>	Подія виникає, якщо у користувача або групи користувачів було видалене певне право	!
Изменение политики	612	Зміна політики аудиту Нова політика: Успіх Відмова <...> <...> Вхід/Вихід <...> <...> Доступ до об'єктів <...> <...> Використання прав <...> <...> Керування обліковими записами <...> <...> Зміна політики <...> <...> Системні події <...> <...> Детальне відстеження <...> <...> Доступ до служби каталогів <...> <...> Вхід через обліковий запис Виконавець: Користувач: <...> Ім'я домену: <...> Код входу: <...>	Подія виникає, якщо була змінена політика аудиту Windows	!
Учетные записи	624	Створення облікового запису користувача Ім'я нового облікового запису: <...> Новий домен: <...> Код облікового запису: <...> Виконавець: <...> Домен виконавця: <...> Код входу виконавця: <...> Привілеї: <...>	Подія виникає, якщо був створений новий обліковий запис користувача Подія виникає, якщо системний адміністратор або адміністратор безпеки створив новий обліковий запис у Windows	?
Учетные записи	630	Видалення облікового запису користувача Ім'я облікового запису: <...> Домен: <...> Код облікового запису: <...> Виконавець: <...> Домен виконавця: <...> Код входу виконавця: <...> Привілеї: <...>	Подія виникає, якщо був видалений обліковий запис користувача Подія виникає, якщо системний адміністратор або адміністратор безпеки видалив обліковий запис Windows	?
Учетные записи	635	Створення локальної групи Ім'я нового облікового запису: <...> Новий домен: <...> Код нового облікового запису: <...> Виконавець: <...> Домен виконавця: <...> Код входу виконавця: <...> Привілеї: <...>	Подія виникає, якщо була створена нова локальна група	!

Категорія	Код	Опис (українською мовою)	Пояснення	
Учетные записи	636	Внесення члена локальної групи Член: <...> Ім'я облікового запису: <...> Домен: <...> Код облікового запису: <...> Виконавець: <...> Домен виконавця: <...> Код входу виконавця: <...> Привілеї: <...>	Подія виникає, якщо до локальної групи був внесений обліковий запис користувача або глобальної групи Подія виникає в результаті зміни адміністратором безпеки ролей користувачів за допомогою програми *Керування захистом*	?
Учетные записи	637	Видалення члена локальної групи Член: <...> Ім'я облікового запису: <...> Домен: <...> Код облікового запису: <...> Виконавець: <...> Домен виконавця: <...> Код входу виконавця: <...> Привілеї: <...>	Подія виникає, якщо з локальної групи був видалений обліковий запис користувача або глобальної групи Подія виникає в результаті зміни адміністратором безпеки ролей користувачів за допомогою програми *Керування захистом*	?
Учетные записи	638	Видалення локальної групи Ім'я облікового запису: <...> Домен: <...> Код облікового запису: <...> Виконавець: <...> Домен виконавця: <...> Код входу виконавця: <...> Привілеї: <...>	Подія виникає, якщо була видалена локальна група	!
Учетные записи	640	Зміна загальної бази даних облікових записів Тип зміни: <...> Тип об'єкта: <...> Ім'я об'єкта: <...> Код об'єкта: <...> Виконавець: <...> Домен виконавця: <...> Код входу виконавця: <...>	Подія виникає у випадку зміни бази облікових записів, не пов'язаної із коригуванням облікових записів	!
Учетные записи	643	Зміна політики для домену: зміна <...> Домен: <...> Код домену: <...> Виконавець: <...> Домен виконавця: <...> Код входу виконавця: <...> Привілеї: <...>	Подія виникає, якщо була змінена політика облікових записів	!

[1]У тому випадку, коли встановлений лише аудит змін дозволів на доступ до файлу чи папки, у журналі можуть з'являтись записи аудиту із зазначенням у переліку видів доступу значення *WRITE_DAC*, хоча зміна дозволів і не мала місця. Наприклад, це відбувається після перегляду (без внесення змін) переліку дозволів на доступ до файлу чи папки за допомогою програми *explorer.exe* (*Проводник*).

Аналогічно, у випадку перегляду значення параметра реєстру за допомогою, наприклад, програми *regedit.exe,* у журналі може з'явитись запис про зміну дозволів (використання програми *regedt32.exe*, яка входить до складу Windows 2000, не дає такого ефекту).

ДОДАТОК Г. Форми звіту про небезпечні події та протоколу друку

Звіт про небезпечні події

За _____(дата)

Час початку роботи: _____

Протягом дня в системі:

зафіксовані небезпечні події:
<перелік подій (зазначаються джерело, ідентифікатор та час події)>;

у тому числі помилки:
<перелік подій (зазначаються джерело, ідентифікатор та час події)>;

Звіт сформований: <Дата та час>

Протокол друку документів

За _____(дата)
(з _____ по _____ (інтервал дат))
Комп'ютер: _____

Надруковано документів: _____
(Всього аркушів: _____)

N п/п	Час	Користу-вач	Принтер	Мітка носія даних	Документ			Надруковано	
					Назва	Гриф	Облі-ковий номер	Аркушів в одному примір-нику	Примір-ників

Протокол сформований: _____(Дата та час)

ДОДАТОК Д. Можливі проблеми під час роботи системи та способи їх вирішення

У таблиці Д.1 наведений перелік відомих проблем, які можуть виникнути під час експлуатації системи та описані шляхи їх подолання.

Таблиця Д.1

Короткий опис проблеми	Можливі причини	Спосіб вирішення
Загальні проблеми		
На початку роботи системи виникає помилка під час операції *Відкриття журналу захисту. Монітор захисту* повідомляє про помилку з кодом *87* під час роботи системної функції		Очистити журнали Windows і запропонувати системі повторити операцію
Помилки під час виконання операції *Відкриття бази даних захисту*	Пошкоджений файл із переліком користувачів – *%LOZA%\Security\Safety\ userlist.cds*	Відновити файл із резервної копії і запропонувати системі повторити операцію. Якщо це неможливо, слід спробувати виправити помилку у файлі вручну за допомогою програми *CDSPad* (вона знаходиться в папці *%LOZA%\Lib*)
На початку роботи програма *Starter* видає повідомлення “Процесс сервера не может быть запущен, так как указана неправильная идентификация. Проверьте правильность указания имени пользователя и пароля”	У налаштуваннях *DCOM* невірно вказаний пароль користувача, від імені якого запускається *Сервер безпеки*	За допомогою утиліти *LOZARecover* (вона знаходиться в папці *%LOZA%\Lib*) встановити користувача для запуску системи (або вручну встановити користувачу, від імені якого запускається *Сервер безпеки*, новий пароль і зазначити його в налаштуваннях *DCOM* за допомогою програми *dcomcnfg*)
	У властивостях облікового запису користувача, від імені якого запускається *Сервер безпеки*, встановлена відмітка про необхідність зміни пароля під час наступного входу до системи	За допомогою утиліти *LOZARecover* (вона знаходиться в папці *%LOZA%\Lib*) встановити користувача для запуску системи (або вручну зняти відмітку про необхідність зміни пароля під час наступного входу до системи і встановити відмітку про необмеженість терміну дії пароля)

Короткий опис проблеми	Можливі причини	Спосіб вирішення
Інші проблеми		Якщо проблема закономірно повторюється, слід звернутись до розробників системи та надати докладну інформацію про послідовність дій, які викликають проблему. Бажано також виконати такі дії • створити в розділі реєстру *HKEY_LOCAL_MACHINE\SOFTWARE\NIIavtoprom* параметр *ReportLOZADebugEvents* типу *DWORD* • виконати дії, які викликають проблему • створити копію системного журналу прикладних програм (журнал *Приложения*) • видалити створений параметр реєстру • надіслати створену копію журналу розробнику
Проблеми під час роботи з програмою *Керування захистом*		
Під час спроби додати шаблон до переліку дозволених шаблонів (меню *Конфігурація\Робота з документами\Шаблони та надбудови)* виникає помилка з повідомленням “Неможливо підрахувати контрольну суму файлу... Код помилки 32”	Виконується програма MS Word чи MS Excel	Припинити роботу з програмою MS Word або MS Excel
Проблеми під час роботи з програмою *Захищені документи*		
Помилка під час створення бази документів на розділі жорсткого диску з повідомленням “Неможливо створити базу. System Error. Code: 183. Невозможно создать файл, так как он уже существует”	Розділ жорсткого диска використовувався для документів у попередній інсталяції системи	
Помилка під час відкриття документа з повідомленням “Не можу відключити шаблон ...”	Програма не може відключити шаблон або надбудову, які завантажуються автоматично	Пересвідчитись, що вказаний шаблон або надбудова MS Word та MS Excel, які завантажуються автоматично (їх розміщення визначається налаштуваннями цих програм, звичайно вони містяться в папках *Office\Startup* – для MS Word та *Office\Startup* – для MS Excel) включені до складу дозволених шаблонів та надбудов (програма *Керування захистом*, меню *Конфігурація\Робота з документами\Шаблони та надбудови)*

Короткий опис проблеми	Можливі причини	Спосіб вирішення
Попередження під час відкриття документа з повідомленням “Файл ... не дозволений для використання”	Указаний шаблон або надбудова MS Word та MS Excel не включені до складу дозволених шаблонів та надбудов (програма *Керування захистом*, меню *Конфігурація\Робота з документами\Шаблони та надбудови)*	За необхідності додати файл до відповідного переліку дозволених шаблонів та надбудов (програма *Керування захистом*, меню *Конфігурація\Робота з документами\Шаблони та надбудови)*
Усі інші проблеми	Збій у роботі програм MS Word та MS Excel	1. Закінчити роботу із програмою *Захищені документи*. 2. Пересвідчись, що в переліку процесів, які виконуються в системі, не залишилося процесів *Winword.exe* та *Excel.exe* 3. Якщо ці процеси виконуються, завершити їх
Проблеми під час реєстрації		
Помилка під час спроби зареєструвати систему способом *Прив’язка до електронного ключа* з повідомленням “Не встановлений ключ uaToken”	Не запускається стандартна служба Windows *Смарт-карты* з повідомленням *Отказано в доступе*. У журналі міститься запис про відсутність доступу до розділу реєстру Кале.	Надати користувачу *LOCAL SERVICE* повний доступ до розділу реєстру *HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\ Cryptography\Calais*

Перелік скорочень та позначень

ЛОМ	локальна обчислювальна мережа
ОС	операційна система
ПЗ	програмне забезпечення
ПРД	правила розмежування доступу
ТЗІ	технічний захист інформації
%LOZA%	коренева папка ЛОЗА-2

У наведеній нижче таблиці вказані позначення для видів доступу до об’єктів.

Вид доступу	Скорочення
Базові види доступу	
Адміністрування	A
Виконання	X
Видалення	D
Видалення папки	DF
Друк	P
Експорт	E
Запис власника	WO
Запис даних	WD
Запис додаткових атрибутів	WEA
Запис рівня доступу	WSL
Запис списку аудиту	WAD
Запис списку доступу	WDC
Запис стандартних атрибутів	WA
Збереження в базі документів	SB
Експорт (збереження у файлі)	S
Коригування довідника типів документів	EKD
Перейменування	RN
Перейменування папки	RF
Створення	C
Створення документа	CD
Створення папки	CF
Читання атрибутів доступу	RAA
Читання даних	RD
Читання довідника типів документів	RKD
Читання додаткових атрибутів	REA
Читання стандартних атрибутів	RA
Складені види доступу	
Друк та експорт	E
Запис	W
Керування доступом	AM
Коригування	ED
Коригування, друк та експорт	EE
Повний доступ	F
Читання бази	RB