Товариство з обмеженою відповідальністю
Науково-дослідний інститут
«Автопром»

Система захисту інформації

ЛОЗА™-2

версія 2

редакція 2.5.4

ЗАГАЛЬНИЙ ОПИС СИСТЕМИ

ЛОЗА-2.ПД.01.1

ТОВ НДІ “Автопром”
Київ, 2009

Зміст

1 Загальні положення

1.1 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. Крім цього, до складу системи входять всі засоби, необхідні для створення комплексної системи захисту інформації в автоматизованій системі класу «2», побудованій на основі ЛОМ (згідно з класифікацією, наведеною в документі НД ТЗІ 2.5–005–99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»).

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 такі послуги безпеки:

- довірча конфіденційність – КД-2 (базова довірча конфіденційність);
- адміністративна конфіденційність – КА-2 (базова адміністративна конфіденційність);
- повторне використання об'єктів – КО-0 (повторне використання об'єктів);
- довірча цілісність – ЦД-1 (мінімальна довірча цілісність);
- адміністративна цілісність – ЦА-1 (мінімальна адміністративна цілісність);
- гаряча заміна – ДЗ-1 (модернізація);
- відновлення після збоїв – ДВ-1 (ручне відновлення);
- реєстрація – НР-2 (захищений журнал);
- ідентифікація та автентифікація – НИ-3 (множинна ідентифікація та 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).

1.2 Сервер та робочі станції

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

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

В одноранговій мережі сервером може бути будь-який комп'ютер, в мережі, побудованій на основі доменів – первинний контролер домену. На сервері встановлюється серверна частина системи ЛОЗА-2.

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.

1.3 Базове та функціональне програмне забезпечення

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

- Microsoft Windows 2000 Professional SP-3 (або вище);
- Microsoft Windows XP Professional SP-2 (або вище);
- Microsoft Windows 2000 Server SP-3 (або вище);
- Microsoft Windows Server 2003 SP-2 (або вище).

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

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 комп'ютерах, на яких користувачі працюватимуть з документами, мають бути встановлені Microsoft Word та Microsoft Excel однієї з таких версій:

- Microsoft Word 97 SP-2 та Microsoft Excel 97 SP-2;
- Microsoft Word 2000 SP-3 та Microsoft Excel 2000 SP-3;
- Microsoft Word 2002 (XP) SP-2 (або вище) та Microsoft Excel 2002 (XP) SP-2 (або вище);
- Microsoft Word 2003 та Microsoft Excel 2003;
- Microsoft Word 2007 та Microsoft Excel 2007.

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

2 Порядок роботи системи

2.1 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 в переліку, для всіх робочих станцій застосовується значення з шаблона.

Шаблон робочої станції не застосовується до сервера.

Одразу після інсталяції системи параметри конфігурації набувають значень за умовчанням. Для деяких параметрів передбачено два варіанти 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 також наведені в таблиці А.1 Додатка А.

2.2 Стани системи

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

- робочий стан;
- стан профілактики;
- стан поновлення ПЗ;
- стан відновлення.

Вважається, що система ЛОЗА-2 в 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 *профілактики* призначений для проведення профілактичних робіт, наприклад, тестування комп'ютера або проведення дефрагментації його жорсткого диска.

Стан *поновлення ПЗ* призначений для проведення змін у складі програмного забезпечення, таких як, наприклад, встановлення нової версії прикладної програми, доповнень до операційної системи та ін.

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

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. 2.3. Правила завершення роботи наведені нижче в п. 0.

Переходи між переліченими вище станами здійснює адміністратор безпеки та/або системний адміністратор за допомогою програми *Монітор захисту* (п. 3.3.3). Система може змінити стан «із власної ініціативи» лише в одному випадку – після виявлення порушень цілісності (п. 4.1).

Під час перебування системи в робочому стані та в стані профілактики виконується автоматична перевірка цілісності програмного середовища (п. 3.4.5). У станах поновлення ПЗ та відновлення перевірка припиняється.

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

Під час виходу зі стану поновлення ПЗ адміністратор має вказати, чи необхідно прийняти зміни в складі програмного середовища. У випадку позитивної відповіді поновлюються відомості про склад програмного середовища. У протилежному випадку проводиться перевірка цілісності, а перехід здійснюється лише у випадку позитивного результату перевірки.

2.3 Початок роботи

На кожному комп'ютері система ЛОЗА-2 починає роботу під час завантаження операційної системи. Стан, у який система намагається перейти на початку роботи, називається *початковим*. Вибір початкового стану відбувається за такими правилами:

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

У протилежному випадку діють наведені нижче правила.

б) Якщо в попередньому сеансі роботи відбулось звичайне завершення роботи, система намагається почати роботу

– у стані, який вказав адміністратор безпеки за допомогою програми *Монітор захисту* як початковий стан для наступного сеансу роботи;

– у стані, у якому відбулось завершення роботи, якщо адміністратор не вказав початковий стан.

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

г) Якщо в попередньому сеансі робота була завершена некоректно, система обирає початковий стан у залежності від значення параметра конфігурації `перехід у стан профілактики після некоректного завершення роботи`. Якщо цей параметр має значення *Так*, система намагається почати роботу в стані *профілактики*, у

протилежному випадку початковий стан обирається за тими ж правилами, що й після звичайного завершення роботи.

2.4 Завершення роботи

Завершення роботи системи на сервері та на робочій станції може бути звичайним, аварійним або некоректним.

Звичайне завершення роботи може бути викликано такими подіями:

а) Параметр `завершувати роботу автоматично` має значення *Так* і відповідно до розпорядку роботи настав час завершення роботи. Час завершення роботи визначається параметрами конфігурації `кінець робочого дня`, `кінець робочого тижня` та `кінець робочого дня наприкінці тижня`.

б) Адміністратор ініціював завершення роботи за допомогою програми *Монітор захисту*.

в) Було здійснено завершення роботи ОС за допомогою засобів Windows.

Варіанти а) та б) можливі лише на сервері.

У випадку виявлення порушення цілісності під час перебування системи в робочому стані або в стані профілактики, система здійснює *аварійне* завершення роботи (якщо це визначено параметром конфігурації `реакція на порушення цілісності` – п. 4.1).

Під час звичайного (випадки а) та б)) та аварійного завершення роботи користувачі впродовж часу, який визначається відповідними параметрами конфігурації (для звичайного завершення – `тривалість видачі попереджень про звичайне завершення роботи`, для аварійного – `тривалість видачі попереджень про аварійне завершення роботи`), отримують попередження про необхідність закінчити роботу. Інтервал між попередженнями визначається параметром конфігурації `періодичність видачі попереджень про завершення роботи`. 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*.

2.5 Автономний режим роботи робочих станцій

Для того щоб забезпечити можливість використання робочих станцій у випадку відсутності зв'язку із сервером, використовується параметр конфігурації `дозволяти вхід до Windows за відсутності зв'язку із сервером`. У цьому режимі запуск програмних засобів системи ЛОЗА-2 неможливий.

Для автентифікації користувачів та керування роботою робочої станції використовуються дані, які були збережені на робочій станції під час останнього сеансу зв'язку із сервером.

2.6 Поновлення програмного забезпечення робочих станцій

Для того щоб спростити процедуру поновлення програмного забезпечення системи, передбачений режим автоматичного поновлення програмного забезпечення робочих станцій.

Автоматичне поновлення програмного забезпечення означає, що на початку роботи робочої станції встановлене на ній програмне забезпечення, яке входить до складу системи ЛОЗА-2, порівнюється із еталоном, який знаходиться на сервері. У випадку виявлення відмінностей необхідні програмні модулі копіюються з сервера на

робочу станцію і за необхідності, після видачі відповідного повідомлення, виконується перезавантаження робочої станції.

Автоматичне поновлення програмного забезпечення робочої станції виконується тільки в тому випадку, коли для цієї станції встановлено значення *Так* для параметра `автоматично поновлювати програмне забезпечення`. За умовчанням цей параметр має значення *Ні*, його значення може бути змінене одночасно для всіх робочих станцій за допомогою шаблона робочої станції (див. п. 2.1).

2.7 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).

У таблиці 1.2.1 наведений повний перелік операцій із короткими поясненнями. До операцій віднесені лише дії, які в разі виникнення помилок потребують втручання адміністратора, тому, наприклад, автоматичні перевірки цілісності програмного середовища, які здійснюються під час перебування системи в робочому стані та в стані профілактики, операціями не вважаються. Тут і далі %LOZA% позначає кореневу папку системи ЛОЗА-2.

Таблиця 1.2.1

Операція	Пояснення	Час виконання
Аналіз попереднього завершення роботи	Визначення початкового стану для чергового сеансу роботи	На початку роботи
Блокування знімних дисків	Обмеження доступу до знімних носіїв (п. 3.4.1.5). Виконується на початку роботи	На початку роботи
Видалення старих звітів та копій журналу захисту	Видалення старих звітів та копій журналу захисту, які підлягають видаленню згідно з відповідними параметрами конфігурації – п. 5.1.5	На початку роботи
Видалення тимчасових файлів	Видалення всіх папок та файлів, які знаходяться в папці %LOZA%\SysTemp, а також у папках, визначених параметром `перелік тимчасових папок` (п. 3.4.4)	На початку роботи, під час виходу зі стану відновлення, під час завершення роботи ОС та після виходу користувача із системи
Відкриття бази даних захисту	Відкриття переліку користувачів	На початку роботи та під час виходу зі стану відновлення
Відкриття журналу захисту		На початку роботи
Завершення роботи	Завершення роботи операційної системи	Під час аварійного завершення роботи

Операція	Пояснення	Час виконання
Запис нового складу завантажувальних секторів	Запис нових характеристик завантажувальних секторів для подальших перевірок цілісності	Після відповідної команди адміністратора
Запис нового складу облікових записів	Запис нових характеристик облікових записів для подальших перевірок цілісності	—”—
Запис нового складу розділів та параметрів реєстру	Запис нових характеристик розділів та параметрів реєстру для подальших перевірок цілісності	—”—
Запис нового складу файлів та папок	Запис нових характеристик файлів та папок для подальших перевірок цілісності	—”—
Запис службової інформації	Запис інформації про останній сеанс роботи до файлу %LOZA%\Security\Server\ LastSession.###	Під час роботи
Зміна паролів прикладних програм	Зміна паролів прикладних програм системи ЛОЗА-2. Ці паролі використовуються для автентифікації програм	На початку роботи
Очищення журналу захисту		Після відповідної команди адміністратора. Така команда може використовуватись тільки як засіб обробки помилок, що виникають під час виконання операції *Відкриття журналу захисту*
Перевірка безпеки середовища	Перевірка настройок ОС, пов’язаних із входом до системи (п. 3.4.2)	На початку роботи та під час виходу зі стану відновлення
Перевірка цілісності завантажувальних секторів	Перевірка цілісності завантажувальних секторів	На початку роботи, під час виходу зі стану відновлення, під час виходу зі стану поновлення ПЗ (якщо адміністратор не підтверджує необхідність прийняти зміни) та після відповідної команди адміністратора
Перевірка цілісності облікових записів	Перевірка цілісності облікових записів	—”—
Перевірка цілісності розділів та параметрів реєстру	Перевірка цілісності розділів та параметрів реєстру	—”—

Операція	Пояснення	Час виконання
Перевірка цілісності файлів та папок	Перевірка цілісності файлів та папок	—”—
Прийняття змін у складі завантажувальних секторів	Запис характеристик змінених завантажувальних секторів для подальших перевірок цілісності	Під час виходу зі стану поновлення ПЗ або після відповідної команди адміністратора
Прийняття змін у складі облікових записів	Запис характеристик змінених облікових записів для подальших перевірок цілісності	—”—
Прийняття змін у складі розділів та параметрів реєстру	Запис характеристик змінених розділів та параметрів реєстру для подальших перевірок цілісності	—”—
Прийняття змін у складі файлів та папок	Запис характеристик змінених файлів та папок для подальших перевірок цілісності	—”—
Створення звіту про небезпечні події	Формування звіту про небезпечні події, його друк та/або збереження у вигляді файлу	У разі виникнення важливих подій – п. 5.1.4.2.1
Читання конфігурації	Читання значень параметрів конфігурації	На початку роботи та під час виходу зі стану відновлення

2.8 Обробка помилок

Під час роботи ядра системи можливе виникнення різноманітних помилок, таких як відсутність параметра реєстру, неможливість доступу до файлу і т. ін. 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 аудита 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 або в стані профілактики, вважається, що була порушена цілісність, і подальша поведінка системи визначається правилами, викладеними в п. 4.1.

в) Якщо помилка була виявлена під час виконання однієї з визначених у системі операцій (п. 2.5), 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 розділу реєстру, 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.

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.

У таблиці 1.2.2 вказано, для яких операцій до переліку включаються пункти *Ігнорувати* та *Відмінити* (вони відмічені знаком «+»), і наведені короткі пояснення.

Таблиця 1.2.2

Операція	Можливі реакції на помилку	
	Ігнорувати	Відмінити
Аналіз попереднього завершення роботи	–	–
Блокування знімних дисків	–	–
Видалення старих звітів та копій журналу захисту	–	+
Видалення тимчасових файлів	–	+
Відкриття бази даних захисту	–	–
Відкриття журналу захисту	+ (очистити журнал захисту)	–
Завершення роботи	–	–
Запис нового складу завантажувальних секторів	–	+
Запис нового складу облікових записів	–	+
Запис нового складу розділів та параметрів реєстру	–	+

Операція	Можливі реакції на помилку	
	Ігнорувати	Відмінити
Запис нового складу файлів та папок	–	+
Запис службової інформації	–	–
Зміна паролів прикладних програм	–	–
Очищення журналу захисту	–	–
Перевірка безпеки середовища	+ (відновити безпеку середовища та перезавантажити ОС)	–
Перевірка цілісності завантажувальних секторів	–	+ (окрім перевірки на початку роботи)
Перевірка цілісності облікових записів	–	+ (окрім перевірки на початку роботи)
Перевірка цілісності розділів та параметрів реєстру	–	+ (окрім перевірки на початку роботи)
Перевірка цілісності файлів та папок	–	+ (окрім перевірки на початку роботи)
Прийняття змін у складі завантажувальних секторів	–	+
Прийняття змін у складі облікових записів	–	+
Прийняття змін у складі розділів та параметрів реєстру	–	+
Прийняття змін у складі файлів та папок	–	+
Створення звіту про небезпечні події	–	+
Читання конфігурації	+ (прийняти для параметра конфігурації значення за умовчанням)	–

2.9 Поведінка системи

Згідно із правилами, викладеними в пп. 2.2 – 2.4, 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;
– чекання перед виходом зі стану (перед виходом зі стану система чекає, доки користувач закінчить роботу);
– здійснення звичайного завершення роботи;

– здійснення аварійного завершення роботи.

Можливість виконання користувачами тих чи інших дій залежить від поточного режиму роботи системи та стану, у якому вона перебуває. Наприклад, працювати з документами можна тільки під час перебування системи в робочому стані, встановлювати значення параметрів конфігурації – тільки під час перебування системи в певному стані та чекання перед виходом зі стану. У випадку неможливості виконання дії користувач отримує повідомлення «Виконання дії в поточний момент неможливе».

3 Керування доступом

3.1 Користувачі системи

3.1.1 Облікові записи системи ЛОЗА-2

Для кожного користувача системи за допомогою програми *Керування захистом* створюється обліковий запис. Сукупність облікових записів утворює *перелік користувачів системи* – єдину складову *бази даних захисту*. 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;
– 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. 3.1.1.1);
– рівень допуску користувача (п. 3.1.1.2);
– відомості про ключовий диск (ключові диски) користувача (п. 3.1.3).

Під час створення облікового запису рекомендується встановити вимогу зміни пароля при наступному вході до системи. Користувач повинен буде змінити пароль при першій же реєстрації в 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. 3.1.4.2), адміністратор не має такої можливості.

Кожний обліковий запис ідентифікується унікальним кодом SID – цей код генерує ОС Windows під час створення облікового запису. Відповідність між обліковими записами системи ЛОЗА-2 та обліковими записами Windows описана нижче, у п. 3.1.2.1.

3.1.1.1 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*.

3.1.1.2 Рівень допуску користувача

Рівень допуску обирається зі стандартного переліку:
- цілком таємно;
- таємно;
- для службового користування;
- відкрита інформація.

Значення в цьому переліку розташовані за спаданням, перше вважається найвищим, останнє – найнижчим.

3.1.1.3 Групи користувачів

Для керування доступом до документів та баз документів використовуються дві групи користувачів, *Всі* та *Адміністратори документів*, а також «віртуальний» користувач *Власник*.

Група *Всі* містить усіх користувачів системи, група *Адміністратори документів* містить усіх користувачів, яким установлена роль *Адміністратор документів*.

Власником бази та документа стає користувач, який їх створює. Застосування «віртуального» користувача *Власник* дозволяє надавати повноваження користувачу під час застосування механізму успадкування (п. 3.2.2.3).

3.1.2 Облікові записи Windows

3.1.2.1 Облікові записи користувачів

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

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.

3.1.2.2 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 3.1. Усі ці групи створюються під час інсталяції системи.

Таблиця 3.1

Ім’я групи	Опис групи	Роль користувача
LOZASecAdmins	Адміністратори безпеки системи ЛОЗА-2	*Адміністратор безпеки*
LOZADocAdmins	Адміністратори документів системи ЛОЗА-2	*Адміністратор документів*

Ім’я групи	Опис групи	Роль користувача
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*.

3.1.2.3 Користувач для запуску системи

Ядро системи – програма *Сервер безпеки* – працює від імені певного користувача Windows. Відповідний обліковий запис створюється під час інсталяції системи. Він додається до групи *LOZAUsers*, вбудованої локальної групи *Администраторы* Windows, а також до групи *LOZASecServers*. Остання група також створюється під час інсталяції системи, і їй надається право входити до системи як пакетне завдання (вход в качестве пакетного задания, logon as a batch job).

Користувач, від імені якого працює ядро системи, називається *службовим*. Для нього не може бути створений обліковий запис у системі ЛОЗА-2.

3.1.3 Ключові диски

Ключові диски використовуються для додаткової автентифікації користувачів системи (п. 3.1.5).

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

Для того щоб диск став ключовим, адміністратор безпеки повинен його ініціалізувати. Під час ініціалізації на диск записується пароль, який (після певного перетворення) запам’ятовується в базі даних захисту. Ініціалізований в одній мережі ключовий диск можна також запам’ятати в базі даних захисту в іншій мережі.

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

Те, які саме диски використовуються як ключові, вказують два параметри конфігурації:

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

Ці параметри можуть приймати такі значення:

- *Не використовувати;*
- *Всі диски;*
- *Вибрані диски* (із зазначенням вибраних дисків).

3.1.4 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.

3.1.4.1 Політика паролів

Політика паролів складається з таких параметрів конфігурації:

– кількість неповторюваних паролів;
– максимальний 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 змушує користувача змінити пароль. 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:

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

3.1.4.2 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 указує 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 указує невірний пароль.

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

3.1.5 Вхід до системи

Правила входу до системи та перевірки ключових дисків визначається такими параметрами конфігурації:

– відображати ім'я попереднього користувача;
– дозволяти вхід до Windows тільки в робочому стані системи;
– перевіряти ключовий диск під час входу до Windows;
– перевіряти ключовий диск під час роботи у Windows;
– дозволяти вхід до Windows за відсутності зв’язку із сервером.

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

Після встановлення системи ЛОЗА-2 починають діяти такі обмеження на роботу користувачів у Windows:

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

– 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;

– буде відключена можливість запуску програм від імені іншого користувача;

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

Якщо параметр `перевіряти ключовий диск під час входу до Windows` має значення ***Так***, увійти до системи та розблокувати комп'ютер можна тільки за наявності ключового диска.

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` визначає, чи відображається ім'я попереднього користувача в діалозі входу до системи ЛОЗА-2.

Якщо для параметра `дозволяти вхід до Windows тільки в робочому стані системи` встановлене значення ***Так***, звичайні користувачі та адміністратори документів зможуть увійти до Windows тільки під час перебування системи ЛОЗА-2 в робочому стані.

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.

Додаткові обмеження на роботу користувачів може накладати параметр `примусово завершувати сеанси роботи під час виходу із робочого стану`. Якщо він має значення ***Так***, сеанси роботи звичайних користувачів та адміністраторів документів будуть примусово завершені під час виходу системи (на сервері або на робочій станції) з робочого стану. Для завершення роботи їм буде наданий час, який визначається параметром `тривалість видачі попереджень про аварійне завершення роботи`.

3.2 Об'єкти доступу

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

1) Бази документів.
2) Документи.
3) Дані захисту:

– база даних захисту (перелік користувачів з їхніми атрибутами доступу та даними, необхідними для автентифікації);

– журнал захисту;

– параметри конфігурації системи;

– оперативні дані про роботу системи;

– перелік робочих станцій.

3.2.1 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»).

3.2.1.1 Атрибути бази

Кожна база документів має атрибути, перелічені в таблиці 3.3. Початкові значення атрибутів встановлюються під час її створення.

Таблиця 3.2 – 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. 3.2.1.7)
Власник	Зберігається SID власника бази	Користувач, який створює базу
Максимальний рівень доступу документів	Значення обирається з такого переліку: – Цілком таємно; – Таємно; – Для службового користування; – Відкрита інформація	Вказує користувач, який створює базу
Мінімальний рівень доступу документів	____”____	____”____
Список доступу	п. 3.2.1.5	Користувачу *Власник* встановлюється *Повний доступ* (п. 3.2.1.4)
Список аудита	п. 3.2.1.5	Для групи *Всі* встановлюється аудит відмов для всіх видів доступу та аудит успіхів для таких видів доступу (п. 3.2.1.4): – створення документів; – запис; – керування доступом
Список доступу для документів	п. 3.2.1.6	Для довірчих баз користувачу *Власник* встановлюється *Повний доступ*. Для адміністративних баз користувачу *Власник* встановлюються дозволи на такі види доступу: *коригування, друк та експорт* (п. 3.2.2.2)

Назва	Пояснення	Початкове значення
Список аудита для документів	п. 3.2.1.6	Для групи *Всі* встановлюється аудит відмов для всіх видів доступу та аудит успіхів для таких видів доступу (п. 3.2.2.2): – друк та експорт; – запис власника; – запис рівня доступу; – запис списку доступу; – запис списку аудита
Перелік додаткових атрибутів	Додаткові атрибути, які мають документи бази, та пов'язані із цими атрибутами відомості (п. 3.2.2.1). Після створення бази значення атрибута не може бути змінене	Порожній перелік

3.2.1.2 Довідник типів документів

Кожна база документів має свій довідник типів документів – перелік можливих типів документів (тобто можливих значень атрибута *Тип* для документів бази (п. 3.2.2.1)). Цей довідник може містити, наприклад, елементи *Лист, Наказ, Доповідь* і т. ін. Під час створення бази довідник створюється порожнім. Згодом користувач із відповідними повноваженнями може його коригувати – додавати, видаляти та змінювати записи в довіднику.

3.2.1.3 Власник бази

Власником бази стає користувач, який створює базу.

Власником довірчої бази може бути лише звичайний користувач, власником адміністративної бази – лише адміністратор документів (п. 3.2.1.7).

3.2.1.4 Види доступу до баз

Розрізняють базові та складені види доступу. У таблиці 3.4 наведені визначені в системі базові види доступу до баз документів та необхідні пояснення.

Таблиця 3.3 – Базові види доступу до баз документів

Вид доступу	Пояснення
Читання атрибутів	Читання атрибутів бази
Читання довідників	Читання довідників бази
Читання списку документів	Читання переліку папок бази, списку документів в кожній папці, всіх стандартних та додаткових атрибутів документів, а також рівня доступу кожного документа
Створення папок	
Видалення папок	
Перейменування папок	

Вид доступу	Пояснення
Створення документів	
Коригування довідника типів документів	Видалення/коригування/додавання записів в довіднику типів документів
Запис атрибутів	Запис атрибутів бази, крім атрибутів *Власник*, *Список доступу* та *Список аудита*
Запис власника	
Запис списку доступу	
Запис списку аудита	
Перейменування	
Видалення	

Для зручності керування доступом визначаються наведені в таблиці 3.5 складені види доступу, кожний з яких є поєднанням декількох базових видів доступу.

Таблиця 3.4 – 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

Вид доступу	Складові
Керування доступом	– Читання атрибутів; – Читання довідників; – Читання списку документів; – Запис власника; – Запис рівня доступу; – Запис списку доступу; – Запис списку аудита
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 аудита

3.2.1.5 Список доступу і список аудита

Список доступу бази складається із двох частин – переліку заборон доступу та переліку дозволів на доступ. Елемент кожного із цих переліків має такий вигляд:

<користувач або група> – <вид доступу>.

Види доступу до баз наведені в п. 3.2.1.4.

Список аудита бази – це перелік, кожний елемент якого встановлює аудит певного виду доступу до бази. Елементи політики мають такий вигляд:

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

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

Аудит подій для довірчих баз може бути заборонений політикою документів (п. 3.2.1.8).

3.2.1.6 Список доступу для документів і список аудита для документів

Атрибути *Список доступу для документів* і *Список аудита для документів* визначають списки, які успадковуються під час створення документів у базі (п. 3.2.2.3).

Список доступу для документів складається із двох частин – переліку заборон доступу та переліку дозволів на доступ. Елемент кожного із цих переліків має такий вигляд:

<користувач або група> – <вид доступу>.

Види доступу до документів наведені в п. 3.2.2.2.

Список аудита для документів – це перелік, кожний елемент якого встановлює аудит певного виду доступу до документів. Елементи політики мають такий вигляд:

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

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

Аудит подій для довірчих баз може бути відключений політикою документів (п. 3.2.1.8)

3.2.1.7 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.

3.2.1.8 Політика документів

Робота з документами регламентується декількома параметрами конфігурації системи, які утворюють *політику документів*. Ці параметри і необхідні пояснення наведені в таблиці 3.6.

Таблиця 3.5 – 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
Дозволяти створення довірчих баз	Може приймати значення *Так* та *Ні*. Значення *Ні* означає, що в системі не можуть створюватись довірчі бази

Назва	Пояснення
Максимальний рівень доступу для довірчих баз	Значення для конфігурації «Стандартна безпека» обирається з такого переліку: – Цілком таємно; – Таємно; – Для службового користування; – Відкрита інформація. 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. Значення *Немає* означає, що в системі не можуть створюватись довірчі бази
Реєструвати події для довірчих баз	Вказує, чи здійснюється реєстрація подій для довірчих баз
Примусове маркування документів перед друком та експортом	Вказує, чи буде користувач змушений під час друку та експорту документів із рівнями доступу *Цілком таємно*, *Таємно* та *Для службового користування* вказувати такі реквізити документа як гриф, літер, обліковий номер тощо

3.2.2 Документи

3.2.2.1 Атрибути документів

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

У таблиці 3.7 перелічені стандартні атрибути документа і вказані їхні початкові значення.

Таблиця 3.6 – 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* і т. ін. 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 3.8 містить атрибути доступу документа і їхні початкові значення.

Таблиця 3.7 – 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 такого переліку: – Цілком таємно; – Таємно; – Для службового користування; – Відкрита інформація 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 допуску цього користувача
Список доступу	Має ту ж структуру, що й список доступу для документів бази (п. 3.2.1.6)	Успадковується від бази (п. 3.2.2.3)
Список аудита	Має ту ж структуру, що й список аудита для документів бази (п. 3.2.1.6)	Успадковується від бази (п. 3.2.2.3)

3.2.2.2 Види доступу до документів

Розрізняють базові та складені види доступу. У таблиці 3.9 наведені базові види доступу до документів та необхідні пояснення.

Таблиця 3.8 – Базові види доступу до документів

Вид доступу	Пояснення
Читання	Читання власне тексту документа

Вид доступу	Пояснення
Запис даних	Коригування тексту документа, 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 аудита*
Запис власника	
Запис рівня доступу	
Запис списку доступу	
Запис списку аудита	

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

Для зручності керування доступом визначаються наведені в таблиці 3.10 складені види доступу, кожний з яких є поєднанням декількох базових видів доступу.

Таблиця 3.9 – 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 аудита

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 аудита

3.2.2.3 Успадкування атрибутів доступу

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

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

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

3.2.3 Дані захисту

Дані захисту включають:

– базу даних захисту (перелік користувачів з їхніми атрибутами доступу та даними, необхідними для автентифікації);

– журнал захисту;

– параметри конфігурації системи;

– оперативні дані про роботу системи (поточний стан системи, результати перевірок цілісності, перелік користувачів, які в поточний момент працюють у системі, тощо);

– перелік робочих станцій.

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

– диски для зберігання документів;

– дозволи на доступ до даних захисту;

– заборонені програми;

– захищені папки;

– небезпечні команди;

– параметри блокування знімних дисків;

– параметри входу до системи;

– параметри журналу;

– параметри захисту друку та експорту документів;

– параметри ключових дисків;

– параметри перевірки цілісності;

– параметри розпорядку роботи;

– переліки шаблонів та надбудов;
– політика аудита;
– політика блокування облікового запису;
– політика документів;
– політика паролів;
– тимчасові файли.

Склад кожної групи наведений у Додатку А.

Для даних захисту 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 і т. ін.

3.3 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;
– дані захисту.

3.3.1 Доступ до баз документів

3.3.1.1 ПРД для баз із довірчим керуванням доступом

Працювати з довірчими базами можуть лише звичайні користувачі. Можливість доступу визначається списком доступу бази.

Користувач отримує доступ до бази документів, якщо виконуються наведені нижче умови:
– йому встановлена роль *Звичайний користувач*;
– у списку доступу бази йому або групі, до якої він належить, не заборонений цей доступ (тобто користувач або група не вказані в переліку заборон із відповідним видом доступу);
– у списку доступу бази йому або групі, до якої він належить, наданий цей доступ (тобто користувач або група вказані в переліку дозволів із відповідним видом доступу).

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 аудита.

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. 3.3.2.1) встановлюється ще одне правило.

Користувачі, яким встановлена роль *Адміністратор безпеки*, отримують такі види доступу до всіх баз:
- читання списку документів;
- читання атрибутів;
- запис власника.

3.3.1.2 ПРД для баз із адміністративним керуванням доступом

Працювати з адміністративним базами можуть звичайні користувачі та адміністратори документів. Можливість доступу визначається списком доступу бази.

Користувач отримує доступ до бази документів, якщо виконуються наведені нижче умови:
- йому встановлена роль *Звичайний користувач* або роль *Адміністратор документів*;
- у списку доступу бази йому або групі, до якої він належить, не заборонений цей доступ (тобто користувач або група не вказані в переліку заборон із відповідним видом доступу);
- у списку доступу бази йому або групі, до якої він належить, наданий цей доступ (тобто користувач або група вказані в переліку дозволів із відповідним видом доступу).

Власник бази має особливі повноваження щодо доступу до «своєї» 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 аудита.

Крім цього, для адміністративних баз діють такі обмеження.

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

– запис власника;
– запис списку доступу;
– запис списку аудита.

Якщо параметр політики документів (п. 3.2.1.8) *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.

3.3.2 Доступ до документів

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

3.3.2.1 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 та рівнем допуску користувача.

Користувач отримує доступ до документа, якщо виконуються наведені нижче умови.
– рівень допуску користувача не нижчий за рівень доступу документа;
– йому встановлена роль *Звичайний користувач*;
– у списку доступу документа йому або групі, до якої він належить, не заборонений цей доступ (тобто користувач або група не вказані в переліку заборон із відповідним видом доступу);
– у списку доступу документа йому або групі, до якої він належить, наданий цей доступ (тобто користувач або група вказані в переліку дозволів із відповідним видом доступу).

Власник документа має особливі повноваження щодо доступу до «своїх» документів.

Якщо користувачеві встановлена роль *Звичайний користувач*, він є власником документа і його рівень допуску 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 аудита.

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

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

- читання атрибутів доступу;
- запис власника.

3.3.2.2 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 та рівнем допуску 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, звичайні користувачі не мають права керувати доступом до документів.

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

- рівень допуску 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 йому або групі, до якої він належить, не заборонений цей доступ (тобто користувач або група не вказані в переліку заборон із відповідним видом доступу);
- у списку доступу документа йому або групі, до якої він належить, наданий цей доступ (тобто користувач або група вказані в переліку дозволів із відповідним видом доступу).

Якщо користувач є власником бази, у якій міститься документ, 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 аудита.

Додатково, для адміністративних баз діють такі обмеження.

Звичайні користувачі можуть отримати всі види доступу, крім таких:
- читання атрибутів доступу;
- запис власника;
- запис рівня доступу;
- запис списку доступу;
- запис списку аудита.

Якщо параметр політики документів (п. 3.2.1.8) *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.

3.3.2.3 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 документ має рівень доступу *Таємно* або *Цілком таємно* і параметр конфігурації `захищати друк документів паролем` має значення *Так*, користувач отримує доступ на друк документа лише за умови введення паролю на друк.

Якщо документ має рівень доступу *Таємно* або *Цілком таємно* і параметр конфігурації `захищати експорт документів паролем` має значення *Так*, користувач отримує доступ на експорт документа лише за умови введення паролю на експорт.

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.

3.3.3 Доступ до даних захисту

Можливість доступу до даних захисту залежить від значення параметра конфігурації `дозволи на доступ до даних захисту`. Цей параметр визначає

дозволи на читання та запис до кожної зі складових даних захисту, наведених у п. 3.2.3. Для параметрів конфігурації дозволи надаються для груп параметрів. Значення за умовчанням для цього параметра наведене в таблиці А.3 Додатку А. Частина дозволів не може бути змінена (відповідні значення виділені в таблиці сірою заливкою значення). Зокрема, дозволи на доступ до даних захисту може змінювати лише адміністратор безпеки.

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

3.4 Додаткові засоби захисту

3.4.1 Захист документів

3.4.1.1 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.

3.4.1.2 Дозволені шаблони та надбудови

Для роботи із програмами Microsoft Excel та Microsoft Word часто використовуються шаблони та надбудови, які можуть містити параметри сторінки, стилі, макроси, комбінації клавіш панелі інструментів і т. ін. Це можуть бути шаблони, які завантажуються автоматично, шаблони, на основі яких створюються документи, або шаблони та надбудови які підключаються під час роботи, а також шаблони та надбудови COM.

Під час роботи в системі користувачу дозволяється використовувати тільки ті шаблони та надбудови, які були дозволені адміністратором безпеки. Для цього 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.`

3.4.1.3 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 Word, Microsoft WordPad та Microsoft Блокнот.

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

3.4.1.4 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;`
- `компакт-диски для зберігання документів;`
- `знімні диски для зберігання документів;`
- `жорсткі диски для зберігання документів.`

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

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

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

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

Документи зберігаються в кореневій папці зазначеного диска в папці LOZADoc.

Зберігати документи на жорстких дисках (тобто на розділах жорсткого диска) можна лише в тому випадку, коли вони використовують файлову систему NTFS. Дозволи на доступ для папки LOZADoc на жорсткому диску система встановлює таким чином, щоб унеможливити доступ до неї для всіх користувачів системи. Цілісність встановлених дозволів перевіряється під час перевірки цілісності файлів та папок.

Для унеможливлення доступу користувачів до документів, які зберігаються на гнучких дисках, компакт-дисках та знімних дисках, рекомендується блокувати ці диски (п. 3.4.1.5).

3.4.1.5 Блокування знімних дисків

Для унеможливлення безпосереднього доступу звичайних користувачів до даних, які зберігаються на знімних дисках, використовується блокування знімних дисків. Блокування означає, що до диска мають повний доступ (*Полный доступ*) лише члени груп *LOZASysAdmins*, *LOZASecAdmins* та *LOZASecServers*, тобто користувачі, які виконують ролі *Системний адміністратор*, *Адміністратор безпеки* та користувач, від імені якого працює ядро системи. Крім того, повний доступ до диска надається користувачу *Система* (*System*). Звичайні користувачі та адміністратори документів безпосереднього доступу до заблокованого диска не мають. Вони можуть отримати доступ до даних лише за допомогою програми *Захищені документи*.

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

- `блокувати гнучкі диски;`

– `блокувати знімні диски`;
– `блокувати компакт-диски`.

Зміни значення цих параметрів набувають чинності негайно.

3.4.2 Забезпечення безпеки середовища

Система ЛОЗА-2 встановлює деякі (незначні) обмеження на роботу користувачів у Windows. Ці обмеження перелічені нижче.

1) ОС Windows 2000/XP/2003/Vista дозволяють відмінити вимогу натискання комбінації клавіш Ctrl+Alt+Del під час входу до системи. Система ЛОЗА-2 встановлює цю вимогу.

2) ОС Windows 2000/XP/2003/Vista дозволяють користувачу запускати прикладні програми від імені іншого користувача. Система ЛОЗА-2 відключає цю можливість.

3) ОС Windows XP/Vista дозволяє використовувати так званий екран привітання та швидке переключення між користувачами (без виходу користувача із системи). Система ЛОЗА-2 відключає цю можливість.

4) ОС Windows 2000/XP/2003/Vista дозволяють перевести комп'ютер у режими сну (hibernate) та чекання (suspend). Система ЛОЗА-2 забороняє використання цих режимів, оскільки під час виходу із режимів сну та чекання автентифікація проводиться лише у випадку встановлення додаткового параметра, який кожний користувач може встановити для себе індивідуально.

Перевірка настройок, які встановлює система ЛОЗА-2 згідно із пп. 1) – 4), складає зміст операції *Перевірка безпеки середовища*. Якщо під час операції виявляється порушення безпеки, система повідомляє про відповідну помилку. Якщо адміністратор обирає для обробки помилки опцію *Ігнорувати* (п. 2.8), відповідні настройки Windows відновлюються і виконується перезавантаження Windows.

Виконання обмежень, описаних у п. 4), виконується безпосередньо *Сервером безпеки* та службою *LOZAGuard* під час роботи під час роботи.

3.4.3 Захищені папки

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

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

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

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

Для того щоб за допомогою засобів системи ЛОЗА-2 захистити файли, що знаходяться в певній папці (папках), необхідно виконати такі дії:

– створити у Windows локальну групу, яка відповідатиме папці (папкам) і надати дозвіл на доступ до папки (папок) тільки цій групі; звичайно для забезпечення можливості роботи з даними достатньо надати дозвіл на доступ *Изменить*;

– усіх користувачів, яким необхідно працювати з даними відповідної програми, додати до створеної групи;

– встановити для папки (папок) аудит доступу; звичайно досить встановити аудит для таких видів доступу: *Чтение данных*, *Запись данных*, *Дозапись данных, Удаление подпапок и файлов*, *Удаление*.

– додати папку (папки) до переліку захищених папок.

Якщо на комп'ютері використовується декілька додаткових програмних засобів (програма AutoCAD, бухгалтерська програма тощо), зазначені дії необхідно виконати окремо для кожної програми.

Після того як папка додається до переліку захищених папок, до переліку подій, які імпортуються до журналу захисту (п. 5.1.3), додається подія #560 джерела *Security* (подія доступу до об'єктів, яку реєструє Windows) із умовою імпорту, згідно з якою подія імпортується в тому випадку, коли її опис містить рядок із іменем папки. У результаті журнал захисту міститиме всі події доступу до файлів та папок, які містяться в захищеній папці.

3.4.4 Видалення тимчасових файлів

У системі ЛОЗА-2 передбачена можливість автоматичного видалення тимчасових файлів. Для цього передбачені такі 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.

Видалення тимчасових файлів користувача зажди відбувається під час входу користувача до системи, а також під час виходу користувача із системи (у тому числі під час завершення роботи Windows).

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 з шаблонів, що міститься в переліку, видаляються.

Видалення файлів та папок, які визначаються параметрами `перелік тимчасових папок` та `перелік 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.

Для видалення тимчасових файлів користувачів та файлів, які містяться в тимчасових папках, застосовується процедура безповоротного видалення (wipe).

3.4.5 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. 3.2.2.1);

– встановлення аудиту друку документа, що забезпечує докладну реєстрацію подій друку (див. п. 3.2.2.1);

– встановлення пароля на друк (див. п. 3.3.2.3).

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 всім);

– `всім` (друк заборонений всім);

– `всім користувачам системи ЛОЗА-2, крім адміністраторів безпеки`;

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

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

– `спеціальна настройка`.

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

Заборона друку, яка визначається зазначеними параметрами, встановлюється 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*).

4 Забезпечення цілісності програмного середовища

Цілісність програмного середовища підтримується за рахунок перевірок цілісності. Перевірки виконуються автоматично, але в разі необхідності адміністратор може ініціювати будь-яку перевірку за допомогою програми *Монітор захисту*.

4.1 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 пп. 4.2, 4.3 та 4.5.

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. 4.6). 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 та в стані профілактики.

У разі виявлення порушення цілісності система здійснює аварійне завершення роботи (п. 0) 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 станах відновлення та поновлення ПЗ 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 зі 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.

Під час виходу зі стану поновлення ПЗ за бажанням адміністратора може бути сформований новий «відбиток» програмного середовища, який запам’ятовується для подальших перевірок. Якщо адміністратор відмовляється від формування нового «відбитку», вихід зі стану поновлення ПЗ відбувається за тими ж правилами, що й вихід зі стану 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 або в стані поновлення ПЗ ця програма дозволяє також провести перевірку та прийняти зміни в складі програмного середовища.

4.2 Перевірка файлів та папок

4.2.1 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 %LOZA%, яка 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 типів 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.

4.2.2 Характеристики, які перевіряються

Під час формування «відбитка» запам'ятовується перелік папок з їхніми дескрипторами безпеки (для томів NTFS) та перелік файлів з їхніми дескрипторами безпеки (для томів NTFS) і контрольними сумами (п. 4.6).

У результаті перевірки можуть бути виявлені такі порушення цілісності:

- змінені файли;
- нові файли;
- видалені файли;
- змінені дескриптори безпеки файлів;
- нові папки;
- видалення папок;
- змінені дескриптори безпеки папок.

4.3 Перевірка розділів та параметрів реєстру

4.3.1 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 (таблиця А.1 у Додатку А). Видалити цей розділ із переліку неможливо.

4.3.2 Характеристики, які перевіряються

Під час формування «відбитка» запам'ятовується перелік розділів з їхніми дескрипторами безпеки та перелік параметрів з їхніми контрольними сумами (п. 4.6).

У результаті перевірки можуть бути виявлені такі порушення цілісності:

- змінені параметри;
- нові параметри;
- видалені параметри;

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

4.4 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.

4.5 Перевірка облікових записів

4.5.1 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`.

4.5.2 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 (п. 4.6) усіх його властивостей: імені, повного імені, сценарію входу 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.

4.6 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 $1-2^{-n}$, де n позначає розрядність контрольної суми. Для підрахунку обрано $n = 32$, тому відповідна ймовірність дорівнює приблизно 0,99999999976.

5 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.

5.1.1 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 і т. ін. 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 між такими категоріями:

- *робота системи* (початок та завершення роботи системи, зміна стану системи та ін.);
- *цілісність* (виявлення порушень цілісності, прийняття змін та ін.).

5.1.2 Реєстрація дій користувачів

Для реєстрації дій користувачів використовується *журнал захисту* (п. 5.1.3). Відповідні події мають тип *Аудит успіхів* або *Аудит відмов* і реєструються від імені джерела *LOZAAudit*. Вони розподілені на такі категорії:

- *вхід/вихід* (вхід користувачів до системи ЛОЗА-2, зміна пароля користувача, вихід із системи та ін.);
- *робота з програмами* (запуск та завершення роботи прикладних програм системи);
- *керування доступом* (коригування бази даних захисту);
- *керування системою* (зміна стану системи, визначення початкового стану для наступного сеансу роботи та ін.);
- *конфігурація* (читання та зміна значень параметрів конфігурації);
- *робочі станції* (читання та коригування переліку робочих станцій);
- *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.).

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

5.1.3 Журнал захисту

Журнал захисту 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 аудита (п. 5.1.2).

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

- `перелік подій, які імпортуються до журналу захисту`;
- `імпортувати всі помилки`.

Параметр `перелік подій, які імпортуються до журналу захисту` дозволяє для кожного журналу та джерела подій Windows вказати події, які слід імпортувати до журналу захисту. Для кожної події може бути задана довільна кількість умов імпорту. Якщо справджується хоча б одна з умов, подія імпортується. Кожна умова може містити такі елементи:

- тип події;
- ім'я користувача, від імені якого подія була зареєстрована;
- перелік рядків, кожний з яких повинен міститись в описі події;
- перелік рядків, кожний з яких не повинен міститись в описі події.

Рекомендоване значення для параметра `перелік подій, які імпортуються до журналу захисту` (воно встановлюється за умовчанням) наведене в Додатку А.

Якщо параметр `імпортувати всі помилки` має значення *Так*, усі події з журналів Windows, які мають тип *Помилка*, імпортуються до журналу захисту (незалежно від того, чи зазначені вони в параметрі `перелік подій, які імпортуються до журналу захисту`).

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

Журнал захисту зберігається у файлі %LOZA%\Security\Log\SecLog\seclog.lzl. Граничний розмір цього файлу визначається параметром конфігурації `граничний розмір журналу захисту`. Після досягнення граничного значення нові події записуються замість старих.

Для збереження зареєстрованих раніше подій здійснюється резервне копіювання журналу захисту. Резервні копії зберігаються в папці %LOZA%\Security\Log\Backup. 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 в певний день. Остання резервна копія знаходиться у файлі *Last.lzl*. Усі події, які реєструються в журналі захисту, одночасно дублюються в цьому файлі. Адміністратор може настроїти систему таким чином, що старі резервні копії журналу захисту будуть поступово видалятись (п. 5.1.5).

Для роботи з журналом захисту 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.

5.1.4 Небезпечні події

5.1.4.1 Перелік небезпечних подій

Деякі з подій, що фіксуються в журналі захисту, 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 має ту ж структуру, що й параметр перелік подій, які імпортуються до журналу захисту (п. 5.1.3).

Якщо другий параметр має значення *Так*, усі події, зареєстровані в журналі захисту 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 захисту. Тому події, зазначені в параметрі перелік небезпечних подій, але не зазначені в параметрі перелік подій, які імпортуються до журналу захисту, небезпечними не вважатимуться. Крім того, події джерела *LOZAAudit*, які не імпортуються, а реєструються в журналі захисту 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.

5.1.4.2 Реакція на небезпечні події

У системі передбачені три способи реагування на небезпечні події:

– створення звіту про небезпечні події;
– звукова сигналізація;
– зміна стану системи.

Система реагує лише на ті небезпечні події, які реєструються в журналі захисту під час роботи системи. Небезпечні події, імпортовані під час перегляду журналів Windows на початку роботи системи (п. 5.1.3), не викликають реакції.

5.1.4.2.1 Звіт про небезпечні події

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

Впродовж одного сеансу роботи 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 сеансу роботи 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*).

5.1.4.2.2 Звукова сигналізація

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

5.1.4.2.3 Зміна стану

Якщо параметр конфігурації `змінювати стан після небезпечної події` має значення *Перехід у стан профілактики* або *Перехід у стан відновлення*, одразу після реєстрації в журналі захисту небезпечної події система перейде в указаний стан. Перехід відбувається лише в тому випадку, коли під час реєстрації небезпечної події система перебуває в робочому стані.

5.1.5 Видалення старих звітів та копій журналу захисту

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

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

Перший параметр визначає, чи відбувається автоматичне видалення копій журналу захисту та звітів, 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).

5.1.6 Протоколи роботи системи

На підставі подій, зареєстрованих у журналі захисту, 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 секретності 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 та ін.).

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

5.1.7 Політика аудита 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 аудита визначає, які із цих дій підлягають реєстрації.

Політика аудита системи ЛОЗА-2 визначається однойменним параметром конфігурації (параметр `політика аудита`) і стосується лише подій, які належать до джерела *LOZAAudit*. Аудит встановлюється для категорій подій, наведених у п. 5.1.2:

- вхід/вихід;
- робота з програмами;
- керування доступом;
- керування системою;
- конфігурація;
- робочі станції;
- доступ до документів;
- доступ до баз документів.

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. 3.2.1.5, 3.2.2.1)

Значення за умовчанням для параметра `політика аудита` наведене в Додатку А.

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 програмним забезпеченням системи ЛОЗА-2

У цьому додатку наведений повний перелік подій, які реєструються програмними засобами системи ЛОЗА-2 у журналі захисту 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 аудита 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 аудита. Можлива втрата деяких результатів аудита. Кількість відхилених повідомлень аудита: <...>	Подія виникає в разі збою під час здійснення аудита, що призводить до втрати частини записів аудита	!
Системное событие	517	Очищення журналу аудита 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 аудита 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 аудита 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 аудита 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 аудита 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		
Під час першого запуску клієнтської частини системи на робочій станції видається повідомлення про неможливість встановлення зв'язку із сервером, яке містить рядок «RPC сервер не доступен»	Проблема викликана роботою брандмауера Windows на сервері	До переліку виключень брандмауера на сервері додати програму *Сервер безпеки* (%LOZA%\Security\Server\ LOZASec.exe)
Немає зв'язку між компонентами системи, розташованими на робочій станції, та сервером. Під час спроби увійти до системи на робочій станції видається повідомлення, яке містить рядок «RPC сервер не доступен» або «Interface not supported»	DCOM (стандартна компонента Windows) не може встановити зв'язок між комп'ютерами. Це може бути викликано декількома причинами	
	Невірно встановлені дозволи на доступ до DCOM на сервері	На сервері запустити програму *Відновлення системи ЛОЗА-2* (%LOZA\Lib\LOZARecover.exe) та виконати дію *Додати дозволи для DCOM*
	Невірно настроєні параметри безпеки Windows на сервері	За допомогою оснащення *Администрирование\Локальная политика безопасности* встановити значення *Включен* для параметра безпеки *Сетевой доступ: разрешать применение разрешений для всех к анонимным пользователям* (це значення встановлюється під час інсталяції системи)
	Роботі DCOM перешкоджає встановлений на сервері брандмауер	Відкрити в брандмауері 135-й порт TCP. Якщо зв'язок не з'явиться, необхідно буде відкрити щ якийсь порт TCP. Щоб визначити його номер, необхідно скористатись журналом брандмауера. Для цього слід встановити параметр *Записывать пропущенные пакеты* в групі *Ведение журнала безопасности* на вкладці *Дополнительно*. Порт, який слід відкрити, буде вказаний в журналі в стовпчику *dst-port*
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

Короткий опис проблеми	Можливі причини	Спосіб вирішення
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 настройках DCOM невірно вказаний пароль користувача, від імені якого запускається *Сервер безпеки*	За допомогою утиліти *LOZATune* (*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 настройках 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 *LOZATune* (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)
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 та надати йому значення 1 • виконати дії, які викликають проблему • створити копію системного журналу прикладних програм (журнал *Приложения*) • видалити створений параметр реєстру • надіслати створену копію журналу розробнику

Короткий опис проблеми	Можливі причини	Спосіб вирішення
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*		
Після час запуску програми на робочій станції і натискання кнопки *Створити/Відкрити* видається повідомлення *Сервер RPC недоступен*	Проблема викликана роботою брандмауера Windows на сервері	До переліку виключень брандмауера на сервері додати програму *Сервер документів* (%LOZA%\Servers\Doc LOZADocSrv.exe)
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 настройками 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)*
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)*
Інші проблеми	Збої у роботі програми MS Word та MS Excel	1. Закінчити роботу із програмою *Захищені документи*. 2. Пересвідчись, що в переліку процесів, які виконуються в системі, не залишились процеси *Winword.exe* та *Excel.exe* 3. Якщо ці процес виконуються, припинити їх

Короткий опис проблеми	Можливі причини	Спосіб вирішення
Проблеми на робочих станціях		
На початку роботи виводиться повідомлення про неможливість встановити зв’язок із сервером безпеки, після чого майже одразу виводиться повідомлення про те, що зв’язок із сервером безпеки встановлено	Зв’язок не встановлюється із «першої спроби» через низьку швидкодію комп’ютерної мережі	Створити на робочій станції в розділі реєстру HKEY_LOCAL_MACHINE\SOFTWARE\NIIavtoprom\LOZA-2 параметр PingTimeout типу DWORD та надати йому значення від 2 до 10 (чим більше значення, тим довше робоча станція намагається встановити зв’язок із сервером). Після цього система зафіксує порушення цілісності реєстру, яке адміністратору безпеки слід прийняти

Перелік скорочень та позначень

ОС	операційна система
ЛОМ	локальна обчислювальна мережа
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 аудита	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