Товариство з обмеженою відповідальністю
Науково-дослідний інститут
”Автопром”

Система захисту інформації

ЛОЗА™-1

версія 3.1.2

ЗАГАЛЬНИЙ ОПИС СИСТЕМИ

ЛОЗА-1.ПД.01.1

ТОВ НДІ “Автопром”
Київ, 2010

Зміст

1 Призначення системи

Система ЛОЗА-1 – це комплекс програмних засобів, призначений для захисту від несанкціонованого доступу інформації, яка міститься в текстових документах та електронних таблицях.

Система також забезпечує захист будь-яких інших даних – на рівні папки операційної системи для даних, які зберігаються на жорсткому диску, та на рівні розділу диска – для даних, які зберігаються на знімних дисках.

Система ЛОЗА-1 містить засоби, необхідні для побудови комплексної системи захисту інформації в автоматизованих системах класу "1" (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-1 надає послуги безпеки, зазначені в таблиці 1.1.

Таблиця 1.1 Профіль системи

Назва послуги		Рівень надання послуги	
		Позначення	Назва
Конфіденційність			
Довірча конфіденційність		КД-2	Базова довірча конфіденційність
Адміністративна конфіденційність		КА-2	Базова адміністративна конфіденційність
Повторне використання об'єктів		КО-0	Повторне використання захищених об'єктів
Цілісність			
Довірча цілісність		ЦД-1	Мінімальна довірча цілісність
Адміністративна цілісність		ЦА-1	Мінімальна адміністративна цілісність
Доступність			
Гаряча заміна		ДЗ-1	Модернізація
Відновлення після збоїв		ДВ-1	Ручне відновлення
Спостереженість			
Реєстрація		НР-2	Захищений журнал
Ідентифікація та автентифікація	«Стандартна безпека»	НИ-2/НИ-3*	Множинна ідентифікація і автентифікація
	«Підвищена безпека»	НИ-3	Одиночна ідентифікація і автентифікація
Достовірний канал		НК-1	Однонаправлений достовірний канал
Розподіл обов'язків		НО-2	Розподіл обов'язків адміністраторів
Цілісність комплексу засобів захисту		НЦ-2	КЗЗ з гарантованою цілісністю
Самотестування		НТ-2	Самотестування при старті

*НИ-2/НИ-3 – рівень надання послуги залежить від значень параметрів конфігурації системи ЛОЗА-1.

Система ЛОЗА-1 може працювати під керуванням таких операційних систем:

- Microsoft Windows XP Professional (Service Pack 2 або вище);
- Microsoft Windows Vista (Service Pack 2 або вище);
- Microsoft Windows 7.

Систему ЛОЗА-1 необхідно встановлювати на диск із файловою системою NTFS.

За рахунок взаємодії з Microsoft Office система ЛОЗА-1 може забезпечити надійний захист документів Microsoft Word та Microsoft Excel. Підтримуються такі версії Microsoft Office:

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

Разом з Microsoft Word та Microsoft Excel має бути встановлена компонента *Visual Basic для приложений*.

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

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

2 Порядок роботи системи

2.1 Параметри конфігурації

Порядок роботи системи ЛОЗА-1 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`.

Одразу після інсталяції системи параметри конфігурації набувають значень за умовчанням. Передбачено два набори значень за умовчанням, а система ЛОЗА-1 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

Для проведення різних видів робіт у системі передбачено два стани:

- робочий стан;
- стан відновлення.

Звичайні користувачі мають доступ до даних лише в *робочому* стані. Цей стан призначений для проведення звичайної роботи системи і в ньому система має перебувати переважну частину часу.

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

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

На початку роботи система автоматично переходить у стан, який визначається за правилами, викладеними в п. 2.3. Правила завершення роботи наведені нижче в п. 2.4.

Переходи між переліченими вище станами здійснює адміністратор безпеки та/або системний адміністратор за допомогою програми *Монітор захисту*. 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 виконується автоматична перевірка цілісності програмного середовища (п. 4). У стані відновлення перевірка припиняється.

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

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

2.3 Початок роботи

Система ЛОЗА-1 починає роботу під час завантаження операційної системи. Стан, у якому починається робота системи, називається *початковим*. Вибір початкового стану залежить від того, яким чином була завершена робота в попередньому сеансі (див. п. 2.4), і відбувається за такими правилами:

а) Якщо в попередньому сеансі роботи відбулось звичайне завершення роботи, початковим є робочий стан.

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

2.4 Завершення роботи

Завершення роботи системи може бути звичайним, аварійним або некоректним.

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

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

Під час аварійного завершення роботи користувач, який працює за комп'ютером, впродовж 5 хв. отримує попередження про необхідність закінчити роботу. Після того як зазначений час мине (або користувач припинить роботу), ініціюється завершення роботи операційної системи.

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

2.5 Операції

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

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

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

2.6 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, 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.

– Повторити.

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

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

1) Відмінити.

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

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

2) 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.

3) 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.

2.7 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-1

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

– ім’я користувача – довільний рядок довжиною до 20 символів, який не може містити символи " / \ [ ] : ; | = , + * ? < > @, а також не може складатись тільки із крапок та пропусків;

– SID (security identifier) користувача, який співпадає з SID’ом відповідного користувача ОС (див. нижче, п. 3.1.2.1);

– повне ім’я користувача (довільний рядок символів);

– опис користувача (довільний рядок символів);

– параметри (вони можуть бути включені або відключені):

  – вимагати зміну пароля при наступному вході до системи;

  – відключити обліковий запис;

  – заблокувати обліковий запис (адміністратор може лише розблокувати обліковий запис, блокує його тільки система);

– пароль (довільний рядок довжиною до 127 символів);

– ролі користувача (п. 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.

Відповідність між обліковими записами системи ЛОЗА-1 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 спрощення керування доступом та аудитом використовуються групи користувачів.

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

Кожна звичайна група має такі атрибути:

– ім’я (довільний рядок символів);
– SID групи – унікальний рядок символів;
– опис (довільний рядок символів);
– перелік облікових записів користувачів – членів групи; тут зберігається перелік SID’ів користувачів.

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

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

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

Звичайно, групи *Власник бази* та *Власник документа* можуть використовуватись лише для керування доступом до документів та баз документів. Група *Власник документа* дозволяє надавати повноваження користувачу під час застосування механізму успадкування (див. п. 3.2.3.3).

Групи користувачів не мають атрибутів доступу.

3.1.2 Облікові записи Windows

3.1.2.1 Облікові записи користувачів

Кожний користувач системи ЛОЗА-1 повинен мати обліковий запис у Windows.

Під час створення облікового запису в системі ЛОЗА-1 адміністратор безпеки може вибрати один з облікових записів Windows (для яких ще не створені облікові записи в системі ЛОЗА-1) або створити новий обліковий запис. Якщо адміністратор створює новий обліковий запис, відповідний обліковий запис буде створений у Windows. Після встановлення властивостей облікового запису системи ЛОЗА-1 встановлюються відповідні властивості облікового запису Windows.

На початку роботи та під час виходу зі стану відновлення система ЛОЗА-1 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-1.

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-1	*Адміністратор безпеки*
LOZADocAdmins	Адміністратори документів системи ЛОЗА-1	*Адміністратор документів*
LOZAOrdinaryUsers	Звичайні користувачі системи ЛОЗА-1	*Звичайний користувач*
LOZASysAdmins	Системні адміністратори системи ЛОЗА-1	*Системний адміністратор*
LOZAUsers	Усі користувачі системи ЛОЗА-1	

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-1.

3.1.3 Ключові диски

Ключові диски використовуються для додаткової автентифікації користувачів системи (п. 3.1.5). На ключовому диску зберігається пароль користувача.

Як ключові диски можуть використовуватись дискети, модулі пам'яті USB Flash та CD/DVD-диски.

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

одному комп’ютері ключовий диск можна також запам’ятати в базі облікових записів на іншому комп’ютері.

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

3.1.4 Політика облікових записів

Політика облікових записів системи ЛОЗА-1 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;
– мінімальний термін дії пароля;
– мінімальна довжина пароля;
– паролі повинні задовольняти вимогам щодо складності.

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

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

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

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

Порядок входу користувачів до системи визначається такими параметрами конфігурації:

- `відображати ім'я попереднього користувача`;
- `перевіряти ключовий диск під час входу до Windows`;
- `перевіряти ключовий диск під час роботи у Windows`
- `дозволяти швидке переключення користувачів`.

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

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

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

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

Значення *Так* параметра конфігурації `перевіряти ключовий диск під час входу до Windows` означає, що увійти до системи та розблокувати комп'ютер можуть тільки ті користувачі, які мають обліковий запис у системі ЛОЗА-1 та, за необхідності, ключовий диск.

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. Значення параметра може бути встановлене тільки у тому випадку, коли для параметра `перевіряти ключовий диск під час входу до Windows` задано значення *Так*.

Параметр `відображати ім'я попереднього користувача` впливає на екран входу до системи. Для Windows XP він визначає, чи відображається ім'я попереднього користувача в діалозі входу до системи ЛОЗА-1. Для Windows Vista/7 цей параметр визначає, чи відображається на екрані перелік користувачів системи.

Параметр конфігурації `дозволяти швидке переключення користувачів` виначає доступність можливості переключення користувачів (тобто входу до системи нового користувача без виходу поперенього). Цей параметр діє тільки в ОС Windows Vista/7, у Windows XP ця можливість відключається одразу після інсталяції системи ЛОЗА-1 і не може бути задіяна.

Від значення параметра `перевіряти ключовий диск під час входу до Windows` залежить рівень надання системою послуги безпеки «Ідентифікація та автентифікація». Якщо для параметра встановлене значення *Так*, послуга надається на

рівні НИ-3 (множинна ідентифікація та автентифікація), якщо встановлене значення *Ні,* послуга надається на рівні НИ-2 (одиночна ідентифікація та автентифікація).

У конфігурації «Підвищена безпека» зазначений параметр завжди має значення *Так*, його значення не може бути змінене.

3.2 Об’єкти захисту

Система ЛОЗА-1 дозволяє захистити інформацію, яка міститься в таких об’єктах:

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

3.2.1 Основні атрибути доступу об’єктів захисту

3.2.1.1 Рівень доступу

Частина об’єктів захисту має рівень доступу. Для всіх об’єктів рівень доступу може приймати ті самі значення, що й рівень допуску користувачів:

- цілком таємно;
- таємно;
- для службового користування;
- відкрита інформація.

3.2.1.2 Списки доступу та списки аудита

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

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

Список доступу можна уявляти собі як перелік елементів такого вигляду:

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

Список аудита – це перелік облікових записів користувачів чи груп користувачів, в якому для кожного облікового запису перелічені всі можливі види

доступу до об’єкта і для кожного виду доступу вказано, чи потрібно реєструвати в журналі реєстрації успішні та неуспішні спроби здійснити цей вид доступу.

Список аудита можна уявляти собі як перелік елементів такого вигляду:

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

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

3.2.2 Бази документів

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

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

3.2.2.1 Атрибути бази

Кожна база документів має атрибути, перелічені в таблиці 3.3. Всі атрибути, крім останніх трьох, є атрибутами доступу. Початкові значення атрибутів встановлюються під час її створення.

Таблиця 3.3 – 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. 3.2.2.5)
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 Значення обмежується політикою документів (п. 3.2.2.6)	Вказує користувач, який створює базу
Мінімальний рівень доступу документів	____“____	____“____
Список доступу	п. 3.2.1.2	Користувачу *Власник* встановлюється *Повний доступ* (п. 3.2.2.4)

Назва	Пояснення	Початкове значення
Список аудита	п. 3.2.1.2 Аудит подій для довірчих баз може бути заборонений політикою документів (див. п. 3.2.2.6).	Для групи *Всі* встановлюється аудит відмов для всіх видів доступу та аудит успіхів для таких видів доступу (п. 3.2.2.4): – створення документів; – запис; – керування доступом
Список доступу для документів	п. 3.2.1.2 Визначає список доступу, який успадковуються під час створення документів у базі (див. п. 3.2.3.3).	Для довірчих баз користувачу *Власник* встановлюється *Повний доступ*. Для адміністративних баз користувачу *Власник* встановлюються дозволи на такі види доступу: *коригування, друк та експорт* (п. 3.2.3.2)
Список аудита для документів	п. 3.2.1.2 Визначає список аудита, який успадковуються під час створення документів у базі (див. п. 3.2.3.3). Аудит подій для довірчих баз може бути заборонений політикою документів (див. п. 3.2.2.6).	Для групи *Всі* встановлюється аудит відмов для всіх видів доступу та аудит успіхів для таких видів доступу (п. 3.2.3.2): – 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. 3.2.3.1). Після створення бази значення атрибута не може бути змінене	Порожній перелік

3.2.2.2 Довідник типів документів

Кожна база документів має свій довідник типів документів – перелік можливих типів документів (тобто можливих значень атрибута *Тип* для документів бази (п. 3.2.3.1)). 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.

3.2.2.3 Власник бази

Власником бази стає користувач, який створює базу.

Власником довірчої бази може бути лише звичайний користувач, власником адміністративної бази – лише адміністратор документів (п. 3.2.2.5).

3.2.2.4 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 3.4 – Базові види доступу до баз документів

Вид доступу	Пояснення
Читання атрибутів	Читання атрибутів бази
Читання довідників	Читання довідників бази
Читання списку документів	Читання папок, списку документів в кожній папці, всіх стандартних та додаткових атрибутів документів, а також рівня доступу кожного документа
Створення папок	
Видалення папок	
Перейменування папок	
Створення документів	
Коригування довідника типів документів	Видалення/коригування/додавання записів 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 3.5 – 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

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

3.2.2.5 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.

3.2.2.6 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 3.6 – 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
Максимальний рівень доступу документів	Значення обирається з такого переліку: – Цілком таємно; – Таємно; – Для службового користування; – Відкрита інформація. Значення цього параметра обмежує вибір значення атрибута бази *Максимальний рівень доступу документів*.
Дозволяти створення довірчих баз	Може приймати значення *Так* та *Ні*. Встановлення значення *Ні* забороняє створення довірчих баз
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
Реєструвати події для довірчих баз	Вказує, чи здійснюється реєстрація подій для довірчих баз
Примусове маркування документів перед друком	Якщо цей параметр має значення *Так*, під час друку документів із рівнем доступу, який визначається параметром `мінімальний рівень доступу для примусового маркування документів`, до тексту документа автоматично додається гриф обмеження доступу документа (у правому верхньому куті). Крім того, для документів із рівнями доступу *Цілком таємно* та *Таємно* користувач отримує можливість вказати додаткові реквізити документа – номер примірника, літер та обліковий номер, – які також будуть внесені до тексту документа

Назва	Пояснення
Мінімальний рівень доступу для примусового маркування документів	Значення обирається з такого переліку: – Цілком таємно; – Таємно; – Для службового користування; – Відкрита інформація. Параметр визначає мінімальний рівень доступу документів, перед друком яких буду здійснюватись примусове маркування

3.2.3 Документи

3.2.3.1 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 3.7 – 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	——“——
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 3.8 – 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	Див. п. 3.2.1.2	Успадковується від бази (п. 3.2.3.3)
Список аудита	Див. п. 3.2.1.2	Успадковується від бази (п. 3.2.3.3)

3.2.3.2 Види доступу до документів

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

Таблиця 3.9 – Базові види доступу до документів

Вид доступу	Пояснення
Читання	Читання тексту документа або електронної таблиці
Запис даних	Коригування тексту документа або електронної таблиці, в тому числі заміна документа (заміна вмісту документа вмістом іншого документа)
Запис стандартних та додаткових атрибутів	
Друк	
Експорт	Збереження документа у вигляді файлу (на жорсткому диску, дискеті чи іншому носії)
Видалення	
Читання атрибутів доступу[1]	Читання атрибутів *Власник*, *Список доступу*, *Список 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 3.10 – 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
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

3.2.3.3 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 групу *Власник документів*. Відповідні повноваження отримує користувач, який створює документ. Після зміни власника ці повноваження отримає новий власник.

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

3.2.4 Захищені папки

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

У таблиці 3.11 перелічені атрибути захищених папок і вказані їхні початкові значення. Всі наведені атрибути є атрибутами доступу. Значення всіх атрибутів вказує адміністратор, який додає папку до списку захищених папок.

Таблиця 3.11 – Атрибути захищеної папки

Назва	Пояснення
Ім’я	Повний шлях до папки
Серійний номер	Зберігається серійний номер диска, на якому знаходиться папка. Використовується номер, який не може бути змінений програмно і однозначно ідентифікує диск
Обмеження для процесів	Значення обирається з такого переліку: – Так; – Ні
Список процесів	Перелік процесів, за допомогою яких користувачі можуть отримати доступ до даних, які зберігаються в захищеній папці
Рівень доступу	Значення обирається з переліку, наведеного в п. 3.2.1.1
Список доступу	Див. п. 3.2.1.2
Список аудита	Див. п. 3.2.1.2

Для кожної захищеної папки за рахунок встановлення значення *Так* для атрибута *Обмеження для процесів* можна дозволити користувачам працювати з захищеними папками та файлами, які знаходяться в них, тільки за допомогою процесів, зазначених в атрибуті *Список процесів*. У цьому списку вказуються шляхи до файлів, що виконуються.

3.2.5 Знімні диски

3.2.5.1 Політика знімних дисків

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

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

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

Кожна політика складається з компонентів, наведених в таблиці 3.12.

Таблиця 3.12 – Політика знімних дисків

Назва	Пояснення
Список доступу	Див. п. 3.2.1.2
Список аудита	Див. п. 3.2.1.2

Політика дисків діє одночасно на всі диски відповідного типу.

3.2.5.2 Зареєстровані диски USB Flash

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

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

Для того щоб встановити атрибути доступу для диска USB Flash, його необхідно додати до списку зареєстрованих дисків. Кожний зареєстрований диск USB Flash має атрибути, наведені у таблиці 3.13. Значення всіх атрибутів вказує адміністратор, який додає диск до списку зареєстрованих дисків.

Таблиця 3.13 – Атрибути зареєстрованого диска USB Flash

Назва	Пояснення
Серійний номер	Зберігається так званий код екземпляру пристрою, який не може бути змінений програмно і однозначно ідентифікує диск
Обмеження для процесів	Значення обирається з такого переліку: – Так; – Ні.
Список процесів	Перелік процесів, за допомогою яких користувачі можуть отримати доступ до даних, які зберігаються на диску
Рівень доступу	Значення обирається з переліку, наведеного в п. 3.2.1.1
Список доступу	Див. п. 3.2.1.2
Список аудита	Див. п. 3.2.1.2

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

3.2.6 Захищені процеси

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

Для захищених процесів визначається один вид доступу – запуск.

У таблиці 3.14 перелічені атрибути захищених процесів і вказані їхні початкові значення. Значення всіх атрибутів вказує адміністратор, який додає процес до списку захищених процесів.

Таблиця 3.14 – Атрибути захищеного процесу

Назва	Пояснення
Ім’я	Шлях до відповідного файлу
Контрольна сума	Контрольна сума відповідного файлу
Список доступу	Див. п. 3.2.1.2
Список аудита	Див. п. 3.2.1.2

3.2.7 Технологічна інформація

До технологічної інформації належать такі дані:

– база облікових записів:

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

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

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

Склад кожної групи наведений у Додатку А.

Для технологічної інформації визначаються два види доступу:

- читання;
- запис.

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

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, її максимальним рівнем доступу, а також роллю та рівнем допуску користувача.

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

– користувачу встановлена роль *Звичайний користувач*;

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

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

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

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

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

– читання списку документів;
– читання атрибутів;
– запис власника;
– запис списку доступу;
– запис списку 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, яке діє для всіх довірчих баз незалежно від списку доступу бази.

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

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

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, її максимальним рівнем доступу, а також роллю та рівнем допуску користувача.

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

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

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

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

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

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

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

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

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

Звичайні користувачі не можуть отримати такі види доступу до бази документів:

– запис атрибутів;
– зміна назви;
– видалення;
– запис власника;
– запис списку доступу;
– запис списку аудита.

Якщо параметр політики документів (п. 3.2.2.6) *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, а також роллю 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*;
– в списку доступу документа користувачу або групі, до якої він належить, не заборонено цей доступ;
– в списку доступу документа користувачу або групі, до якої він належить, надано цей доступ.

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

Якщо користувачу встановлена роль *Звичайний користувач*, він є власником документа і його рівень 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.

Під час створення документів виконується нижченаведене правило.

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

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

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

– читання атрибутів доступу;
– запис власника.

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, а також роллю 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, керувати доступом до документів можуть лише адміністратори 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;
– в списку доступу документа користувачу або групі, до якої він належить, не заборонено цей доступ;

– в списку доступу документа користувачу або групі, до якої він належить, надано цей доступ.

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

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

Якщо користувач є власником бази і йому встановлена роль *Адміністратор документів*, він отримує до документа такі види доступу:
– читання атрибутів доступу;
– запис власника;
– запис рівня доступу;
– запис списку доступу;
– запис списку аудита.

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

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

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

Під час створення документів виконується нижченаведене правило.

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

Якщо параметр політики документів (п. 3.2.2.6) *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 рівень доступу документа не нижчий за значення параметра `мінімальний рівень доступу для використання пароля на експорт документів`, користувач отримує доступ на експорт документа лише за умови введення паролю.

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

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

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

3.3.3 Доступ до захищених папок

3.3.3.1 Загальні правила

Користувач отримує доступ до захищеної папки, якщо виконуються такі умови:
– рівень допуску користувача не нижчий за рівень доступу захищеної папки;
– в списку доступу захищеної папки користувачу або групі, до якої він належить, не заборонено цей доступ;
– в списку доступу захищеної папки користувачу або групі, до якої він належить, надано цей доступ.

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

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

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

3.3.3.2 Доступ до програмних засобів та даних системи ЛОЗА-1

Доступ до файлів, які відповідають програмним засобам системи ЛОЗА-1, а також до файлів, в яких зберігаються дані системи, повинен регулюватись таким же чином, що й доступ до захищених папок. Списки доступу та списки процесів відповідних папок та файлів повинні бути сталими і узгодженими з розподілом функцій між модулями системи та технологією роботи користувачів в системі.

3.3.4 Доступ до знімних дисків

Можливість доступу користувача до зареєстрованого диска USB Flash визначається списком доступу диска, його рівнем доступу та рівнем допуску користувача. Можливість доступу до дисків USB Flash, які не були зареєстровані, а також до гнучких дисків та CD/DVD-дисків визначається відповідною політикою знімних дисків (див. п. 3.2.5.1).

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

– рівень допуску користувача не нижчий за рівень доступу диска;

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

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

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

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

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

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

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

3.3.5 Доступ до захищених процесів

3.3.5.1 Загальні правила

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

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

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

3.3.5.2 Доступ до процесів системи ЛОЗА-1

Процеси, які використовуються для доступу до баз документів, документів та об’єктів, що містять технологічну інформацію, автоматично включаються до списку захищених процесів. Вони мають сталі списки доступу, сформовані відповідно до ролей користувачів такими чином, щоб можливість запуску процесу відповідала наведеній нижче таблиці 3.15. Таблиця відповідає найбільш гранульованому варіанту проектування модулів системи. Якщо ж процес забезпечуватиме доступ одночасно до декількох груп об’єктів, доступ до нього повинні мати усі користувачі, яким цей доступ необхідний.

В таблиці використані такі позначення:

– «+» – користувач може отримати доступ до процесу;
– «–» – користувач не може отримати доступу до процесу.

Таблиця 3.15 – Матриця доступу до процесів

Об'єкти, з якими працює процес / Суб'єкти	Бази документів та документи	База облікових записів	Дані про об'єкти захисту	Дані про бази документів та документи	Журнал реєстрації	Параметри конфігурації	Оперативні дані
Звичайний користувач	+	–	–	+	–	–	–
Адміністратор безпеки	+	+	+	+	+	+	+
Системний адміністратор	–	–	–	–	–	+	+
Адміністратор документів	+	–	–	+	–	–	–

3.3.6 Доступ до технологічної інформації

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

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

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

Для забезпечення можливості керування доступом до об'єктів, що містять технологічну інформацію, використовується параметр конфігурації `дозволи на доступ до технологічної інформації`. Цей параметр визначає дозволи та заборони дозволу на читання та запис до кожної зі складових технологічної інформації, наведених у п. 3.2.7. 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). Зокрема, дозволи на доступ до технологічної інформації може змінювати лише адміністратор безпеки.

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

3.3.7 Ототожнення

У випадку, коли користувачу необхідно працювати з документами, що зберігаються на знімному носії, на декількох комп'ютерах, можливе виникнення ситуації, коли дозволи на доступ до документа або бази документів, надані на одному комп'ютері, не матимуть сили на іншому (незалежно від того чи використовує користувач на різних комп'ютерах одне й те ж ім'я). Причина полягає в тому, що в списках доступу документа та бази документів (які зберігаються разом із документами та базами) зазначається не ім'я користувача, а його унікальний ідентифікатор – SID. Ці ідентифікатори ніколи не повторюються, тому на різних комп'ютерах один і той же

користувач матиме різні SID'и. Для того щоб запобігти такій ситуації і надати користувачам можливість працювати з документами на різних комп'ютерах, використовується *ототожнення* користувачів.

Для кожного користувача системи в базі облікових записів може зберігатись перелік ототожнень – перелік користувачів інших комп'ютерів (точніше, інших інсталяцій Windows), з якими він ототожнений. У переліку ототожнень зберігаються SID'и користувачів.

Ототожнення встановлюються тільки для звичайних користувачів та для адміністраторів документів (роль *Адміністратор документів* може суміщатись з іншими адміністративними ролями).

Для того, щоб встановити ототожнення, необхідно на одному комп'ютері експортувати список користувачів на знімний носій, а потім на іншому комп'ютері для певних користувачі вказати, з ким їх треба ототожнити. Порядок встановлення ототожнень докладно писаний в документі „Інструкція адміністратора безпеки".

Виконання правил розмежування доступу здійснюється з урахуванням ототожнень. Як саме враховуються ототожнення, зручно показати на прикладі. Нижче наведено ПРД для баз із довірчим керуванням доступом (див. п. 3.3.1.1).

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

– користувачу встановлена роль *Звичайний користувач*;

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

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

– у списку доступу бази йому або групі, до якої він належить, наданий цей доступ.

З урахуванням ототожнень це правило набуде такого вигляду:

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

– йому встановлена роль *Звичайний користувач*;

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

– у списку доступу бази цьому користувачу, користувачу, з яким він ототожнений, або групі, до якої він належить, не заборонений цей доступ;

– у списку доступу бази цьому користувачу, користувачу, з яким він ототожнений, або групі, до якої він належить, наданий цей доступ.

Ототожнення стосується також і власника бази, тобто користувач, який став власником бази на одному комп'ютері, може залишатись її власником на іншому комп'ютері за рахунок ототожнення.

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, які можуть містити небезпечні з точки зору захисту макроси. Таку ж небезпеку можуть складати процедури, що містяться в так званих надбудовах (Addins та COM Addins). Для того, щоб надати користувачам можливість використовувати необхідні їм шаблони та надбудови, використовуються такі параметри конфігурації:

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

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

Якщо шаблон або надбудова зазначені в одному з цих параметрів і відповідна контрольна сума не змінилась, вони вважаються безпечними і їх використання дозволяється. Всі інші шаблони та надбудови під час роботи користувача з документами в системі ЛОЗА-1 відключаються.

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 Excel, 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.

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

Документи зберігаються в кореневій папці зазначеного диска в папці LOZADoc. Користувачі системи не мають безпосереднього доступу до цієї папки і отримують доступ до баз документів та документів тільки за допомогою програмних засобів для роботи з документами із складу системи ЛОЗА-1.

3.4.2 Забезпечення безпеки середовища

В тех.проекте не так

Для забезпечення обмежень на роботу користувачів, перелічених в п. 3.1.5 система ЛОЗА-1 відстежує виконання перелічених нижче вимог.

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

2) В ОС Windows XP має бути відключена можливість запускати прикладні програми від імені іншого користувача. В ОС Windows Vista/7 вказана можливість зберігається (див. п. 3.1.5)

3) ОС Windows XP/Vista/7 дозволяють перевести комп'ютер у режими сну (hibernate) та чекання (suspend). Система ЛОЗА-1 забороняє використання цих режимів, оскільки під час виходу із режиму сну автентифікація користувача взагалі не виконується, а під час виходу із стану чекання автентифікація проводиться лише у випадку встановлення додаткового параметра, який адміністратор може не встановити.

Зазначені настройки встановлюється під час інсталяції системи ЛОЗА-1.

Перевірка настройок, які встановлює система ЛОЗА-1 згідно з пп. 1) – **Ошибка! Источник ссылки не найден.**, 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* (див. п. 2.6), відповідні настройки Windows відновлюються і виконується перезавантаження Windows.

Виконання обмежень, описаних в п. 3), виконується безпосередньо *Сервером безпеки* під час роботи (для цього використовується механізм повідомлень Windows – *Сервером безпеки* відповідним певним реагує на повідомлення WM_POWERBROADCAST з параметром PBT_APMQUERYSUSPEND).

3.4.3 Безпечне видалення файлів

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

3.4.3.1 Видалення об'єктів захисту

Система ЛОЗА-1 забезпечує безпечне (без можливості відновлення) видалення файлів, в яких зберігаються такі об'єкти захисту:

– бази документів;
– документи;
– технологічна інформація.

Крім того, під час видалення всіх файлів, які зберігаються у захищених папках, на зареєстрованих знімних дисках, а також на знімних дисках, для яких встановлена політика.

3.4.3.2 Видалення тимчасових файлів

В системі ЛОЗА-1 передбачена можливість автоматичного видалення тимчасових файлів. Для цього передбачені три параметри конфігурації:

- `видаляти тимчасові файли користувачів`;
- `перелік тимчасових папок`;
- `перелік тимчасових файлів`.

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

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

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

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

3.4.4 Заборона друку

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

- встановлення дозволу/заборони друку документа (див. п. 3.2.3.1);
- встановлення аудиту друку документа, що забезпечує докладну реєстрацію подій друку (див. п. 3.2.3.1);
- 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-1, крім адміністраторів безпеки;
- всім користувачам системи ЛОЗА-1, крім адміністраторів документів;
- всім користувачам системи ЛОЗА-1, крім адміністраторів безпеки та документів;
- спеціальна настройка.

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

Заборона друку, яка визначається зазначеними параметрами, встановлюється на початку роботи системи та під час кожного входу користувача до системи.

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 параметра перевіряти ключовий диск під час входу до Windows має значення *Так*). Утиліта надає можливість тимчасово дозволити друк. Адміністратор вказує також «термін дії» тимчасового дозволу на друк, обираючи один з двох варіантів:

– *до заборони друку адміністратором* – це означає, що для відновлення заборони друку адміністратор повинен знову скористатись утилітою *Помічник адміністратора*;

– *поки встановлений ключовий диск адміністратора* (цей варіант доступний лише тоді, коли параметр перевіряти ключовий диск під час входу до Windows має значення *Так*).

4 Перевірка 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. 2.4) або переходить у стан відновлення – в залежності від значення параметра конфігурації `реакція на порушення цілісності`. Якщо здійснюється аварійне завершення роботи, на початку наступного сеансу система потрапляє в стан відновлення.

У стані відновлення постійні та періодичні перевірки не проводяться.

Під час виходу зі стану відновлення для всіх видів об'єктів, для яких зазначена перевірка при старті, знову проводиться перевірка цілісності. Вихід 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..

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

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

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

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

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

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

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

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

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

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

У разі перевищення граничного розміру старі записи видаляються з файлу.

Відомості про останню проведену перевірку можна переглянути за допомогою програми *Монітор захисту*. Під час перебування системи в стані відновлення ця програма дозволяє також провести перевірку та прийняти зміни в складі програмного середовища.

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 оточення Windows, а також рядка %LOZA%, який позначає кореневу папку системи ЛОЗА-1.

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-1, для параметрів `перелік типів файлів для перевірки цілісності`, `перелік папок для перевірки цілісності` та `перелік файлів для перевірки цілісності` визначені обов'язкові елементи (їх не можна видалити під час коригування значень відповідних параметрів). Відповідні відомості наведені в таблиці А.1 у Додатку А.

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;
– видалені папки;
– 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-1 і визначається перевірка вкладених у нього розділів (див. таблицю 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 (див. 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 (див. п. 4.6) усіх його властивостей: імені, повного імені, сценарію входу, домашньої папки та ін.

У результаті перевірки можуть бути виявлені такі порушення цілісності:

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

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.

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

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-1, 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 на категорії, наведені в таблиці 5.1.

Таблиця 5.1 – Категорії подій

Назва	Пояснення
Робота системи	Початок та завершення роботи системи, зміна стану системи та ін.
Цілісність	Виявлення порушень цілісності, прийняття змін та ін.

5.1.2 Реєстрація дій користувачів

Для реєстрації дій користувачів використовується *журнал реєстрації* (див. п. 5.1.3). Відповідні події мають тип *Аудит успіхів* або *Аудит відмов* і реєструються від імені джерела *LOZAAudit*. У разі, коли користувач отримує дозвіл на виконання дії, реєструється подія, яка має тип *Аудит успіхів*, у протилежному випадку – подія, яка має тип *Аудит відмов*. Події джерела *LOZAAudit* розподілені на категорії, наведені в таблиці 5.2.

Таблиця 5.2 – Категорії подій

Назва	Пояснення
Вхід/вихід	Вхід користувачів до системи ЛОЗА-1, зміна пароля користувача, вихід із системи та ін.
Робота з програмами	Запуск та завершення роботи прикладних програм системи
Керування доступом	Коригування бази облікових записів та даних про об’єкти захисту
Керування системою	Зміна стану системи, визначення початкового стану для наступного сеансу роботи та ін.
Конфігурація	Читання та зміна значень параметрів конфігурації

Доступ до документів	Читання, коригування, друк документів, коригування атрибутів доступу документів та ін.
Доступ до баз документів	Читання бази, створення документів, коригування бази та ін.
Доступ до захищених папок	Читання та запис папок та файлів, які знаходяться у захищеній папці
Доступ до знімних дисків	Читання та запис папок та файлів, які знаходяться на диску
Доступ до захищених процесів	Запуск процесу

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

5.1.3 Журнал реєстрації

Журнал реєстрації призначений для того, щоб зібрати в одному переліку всі події, пов'язані з безпекою інформації. Цей журнал формується засобами системи ЛОЗА-1 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. 5.1.7).

Під час роботи системи відбувається аналіз подій, які з'являються в журналах Windows, і частина подій імпортується до журналу реєстрації, 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`;
- `імпортувати всі помилки`.

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

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

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

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

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

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

5.1.4 Небезпечні події

5.1.4.1 Перелік небезпечних подій

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

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

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

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

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

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

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

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

Файли звітів зберігаються 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 реєстрації кожної небезпечної події супроводжується звуковим сигналом, який відповідає стандартній події Windows *Критическая ошибка*.

5.1.4.2.3 Зміна стану

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

5.1.5 Видалення старих звітів та копій журналу

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

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

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

5.1.6 Протоколи роботи системи

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

- протокол друку документів;
- протокол за вибором.

Протокол друку створюється за датою чи інтервалом дат.

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

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

Форма протоколу друку наведена в Додатку Г.

Протокол за вибором створюється за вказаними критеріями відбору (за всіма подіями, за якоюсь подією, за категорією подій, за діями певного користувача 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-1

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-1 визначається однойменним параметром конфігурації (параметр `політика аудита`) і стосується лише подій, які належать до джерела *LOZAAudit*. Аудит встановлюється для категорій подій, наведених у п. 0:

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

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

Аудит доступу до документів та баз документів додатково регулюється списками доступу документів та баз документів (пп. 3.2.2.1 та 3.2.3.1).

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-1, а також різноманітні технічні відомості про параметри конфігурації.

Повний текст додатку міститься у файлі LOZA-1_SecDescr_A.pdf, який знаходиться в папці Doc на дистрибутивному диску системи.

ДОДАТОК Б. Події, які реєструються системою ЛОЗА-1

У цьому додатку наведений повний перелік подій, які реєструються програмними засобами системи ЛОЗА-1 у журналі реєстрації та у журналі прикладних програм Windows.

Повний текст додатку міститься у файлі LOZA-1_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-1 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		
На початку роботи системи виникає помилка під час операції *Відкриття журналу захисту. Монітор захисту* повідомляє про помилку з кодом 87 під час роботи системної функції		Очистити журнали Windows і запропонувати системі повторити операцію
Помилки під час виконання операції *Відкриття бази даних захисту*	Пошкоджений файл із переліком користувачів – %LOZA%\Security\Safety\ userlist.cds	Відновити файл із резервної копії і запропонувати системі повторити операцію. Якщо це неможливо, слід спробувати виправити помилку у файлі вручну за допомогою програми *CDSPad* (вона знаходиться в папці %LOZA%\Lib)
На початку роботи програма *Starter* видає повідомлення “Процесс сервера не может быть запущен, так как указана неправильная идентификация. Проверьте правильность указания имени пользователя и пароля”	У настройках DCOM невірно вказаний пароль користувача, від імені якого запускається *Сервер безпеки*	За допомогою утиліти *LOZARecover* (*вона* знаходиться в папці %LOZA%\Lib) встановити користувача для запуску системи (або вручну встановити користувачу, від імені якого запускається *Сервер безпеки*, новий пароль і зазначити його в 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 *LOZARecover* (вона знаходиться в папці %LOZA%\Lib) встановити користувача для запуску системи (або вручну зняти відмітку про необхідність зміни пароля під час наступного входу до системи і встановити відмітку про необмеженість терміну дії пароля)

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

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

Перелік скорочень та позначень

ОС	операційна система
ПЗ	програмне забезпечення
ПРД	правила розмежування доступу
ТЗІ	технічний захист інформації
%LOZA%	коренева папка ЛОЗА-1

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