

Товариство з обмеженою відповідальністю
**Науково-дослідний інститут
«Автопром»**

Система захисту інформації

ЛОЗА™-1

версія 3.2.0

**ІНСТРУКЦІЯ
СИСТЕМНОГО АДМІНІСТРАТОРА**

ЛОЗА-1.ІЗ.03.3



ТОВ НДІ «Автопром»
Київ, 2012

Зміст

1 Вимоги до апаратного та програмного забезпечення	3
2 Рекомендації з настройки Windows	4
2.1 Параметри безпеки Windows	5
2.1.1 Політика облікових записів.....	5
2.1.2 Політика аудита.....	5
2.1.3 Параметри журналів	6
2.2 Реєстрація подій роботи із принтерами	6
3 Технічні відомості про систему ЛОЗА-1	7
3.1 Склад та розміщення програмного забезпечення системи.....	7
3.2 Відновлення системи ЛОЗА-1	7
3.2.1 Створити локальні групи.....	8
3.2.2 Зробити себе адміністратором безпеки.....	9
3.2.3 Зареєструвати ядро	9
3.2.4 Встановити значення за умовчанням для параметрів конфігурації.....	10
3.2.5 Встановити аудит для файлів та папок.....	10
3.2.6 Встановити дозволи для файлів та папок.....	10
3.2.7 Встановити аудит для розділів реєстру.....	11
3.2.8 Встановити дозволи для розділів реєстру.....	12
3.2.9 Створити змінну оточення %LOZA%	12
3.2.10 Додати дозволи для DCOM.....	12
3.2.11 Встановити принтер для профілю Default	12
Перелік скорочень та позначень	14

1 Вимоги до апаратного та програмного забезпечення

Система ЛОЗА-1 не висуває особливих вимог до апаратного забезпечення комп'ютера. Для встановлення системи необхідно 25 МБ на жорсткому диску. Під час роботи система споживає приблизно 15 МБ оперативної пам'яті.

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 (x86 та x64).

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 приложених*.

Інсталяція системи ЛОЗА-1 докладно описана в документі „Інструкція з інсталяції.”

2 Рекомендації з настройки Windows

В операційних системах Windows XP/Vista/7 передбачені додаткові засоби захисту, які не активізуються після стандартної інсталяції ОС. Використання цих засобів не є необхідним для роботи системи ЛОЗА-1, але є безумовно доцільним, особливо для побудови на основі системи ЛОЗА-1 комплексної системи захисту інформації. Для того щоб активізувати ці засоби, зручно скористатись механізмом шаблонів безпеки.

До складу системи ЛОЗА-1 включений шаблон безпеки *LOZA-1.inf*, який після інсталяції системи знаходитиметься в папці *%LOZA%\Lib* (тут і далі *%LOZA%* позначає кореневу папку системи ЛОЗА-1).

Для того щоб настроїти Windows XP/Vista/7 згідно із шаблоном *LOZA-1.inf*, достатньо запустити програму *Настройка безпеки Windows (%LOZA%\LIB\LOZAWinSec.exe)* та натиснути кнопку *Настроїти* (для застосування шаблону можна використати також стандартні засоби адміністрування Windows).

Шаблон *LOZA-1.inf* отриманий поєднанням стандартних шаблонів *setup_security.inf* та *hiseccws.inf*. До результату поєднання внесені такі зміни:

1) У секції [Privilege Rights] видалений рядок
sebatchlogonright =
(за наявності цього рядка під час застосування шаблону очищається перелік облікових записів, яким надано повноваження *Вход в качестве пакетного задания*).

2) У секції [Registry Values] рядок
machine\software\microsoft\driver signing\policy=3,2
змінений на
machine\software\microsoft\driver signing\policy=3,1
(значення параметра *Устройства: поведение при установке неподписанного драйвера* змінене з *Не разрешать установку на Предупреждать, но разрешать установку*).

Також до секції [Registry Values] доданий рядок
machine\system\currentcontrolset\control\print\providers\eventlog=4,7
(встановлена реєстрація подій роботи з принтерами).

3) Змінені граничні розміри журналів Windows. Для цього встановлені такі значення:

[System Log]
MaximumLogSize = 2048
[Security Log]
MaximumLogSize = 4096
[Application Log]
MaximumLogSize = 2048

Під час застосування шаблону *LOZA-1.inf* встановлюються дозволи на доступ до системних папок та реєстру, змінюються параметри запуску системних служб, а також встановлюються значення для численних параметрів безпеки. Значення, які встановлюються для найбільш важливих параметрів безпеки, описані нижче, у п. 2.1.

Після застосування шаблону *LOZA-1.inf* також встановлюється реєстрація подій роботи з принтером. Відповідні пояснення наведені у п. 2.2.

Для підвищення захищеності рекомендується встановити на комп'ютері лише одну операційну систему (ОС) і за рахунок настройки BIOS Setup унеможливити завантаження ОС із дискети, диска CD-ROM та інших знімних носіїв.

2.1 Параметри безпеки Windows

2.1.1 Політика облікових записів

Під час застосування шаблону *LOZA-1.inf* встановлюються такі значення для параметрів політики облікових записів:

- максимальний термін дії паролю – 42 дні;
- мінімальна довжина паролю – 6 символів;
- паролі повинні відповідати вимогам складності;
- мінімальний термін дії паролю – 0 днів;
- унікальність паролів – 2 пароля;
- блокування облікового запису до зняття блокування адміністратором;
- блокування після 3 невдалих спроб входу;
- поновлення відліку (сброс счетчика) через 30 хвилин.

Встановлення параметра *паролі повинні відповідати вимогам складності* змушує користувачів обирати паролі, які задовольняють нижченаведеним обмеженням.

1) Пароль не повинен містити в собі ім'я користувача чи частину його повного імені.

2) Пароль має містити символи хоча б із трьох наборів із наведених чотирьох:

- прописні літери латинського алфавіту: A,B,C,D,...,Z;
- строкові літери латинського алфавіту: a,b,c,d,...,z;
- цифри: 0,1,2,3,...,9;
- спеціальні символи:

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

Для кожного знов створеного користувача рекомендується залишати відмітку про необхідність зміни пароля під час першого входу до системи, – у результаті пароль користувача знатиме тільки він.

2.1.2 Політика аудита

Під час застосування шаблону *LOZA-1.inf* встановлюється аудит успіхів і відмов для таких категорій (у дужках наведена назва відповідного параметра політики):

- Вхід и выход (Аудит входу в систему);
- Доступ к файлам и объектам (Аудит доступа к объектам);
- Управление пользователями и группами (Аудит управления учетными записями);
- Изменение политики безопасности (Аудит изменения политики);
- Перегрузка, выключение и системные события (Аудит системных событий).

Для категорій *Применение прав пользователей (Аудит использования привилегий)* та *Отслеживание процессов (Аудит отслеживания процессов)* аудит не встановлюється, оскільки відповідні події не містять суттєвих відомостей щодо безпеки інформації, а реєстрація подій категорії *Отслеживание процессов* може, з іншого боку, призвести до захаращення журналу безпеки. Також не встановлюється аудит для категорій *Доступ к службе каталогов (Аудит доступа к службе каталогов)* та *Вход учетной записи (Аудит событий входа в систему)*, оскільки відповідні події не мають сенсу для локальної системи.

2.1.3 Параметри журналів

Під час застосування шаблону *LOZA-1.inf* для журналу системи (*Журнал системы*) та журналу прикладних програм (*Журнал приложений*) встановлюються такі значення:

- *Максимальный размер журнала* – 2048 КБ;
- *Затирать старые события по необходимости*.

Журнал безпеки (*Журнал безопасности*) при встановленому аудиті заповнюється швидше, ніж два інші журнали, тому його параметри встановлюються таким чином:

- *Максимальный размер журнала* – 4096 КБ;
- *Затирать старые события по необходимости*.

2.2 Реєстрація подій роботи із принтерами

Реєстрація подій роботи із принтерами означає, що для встановлених на комп'ютері принтерів у журналі системи реєструються події, пов'язаних із друком документів, а також помилками й попередженнями, які виникають під час друку.

Реєстрацію подій роботи із принтерами можна настроїти вручну. Для цього на вкладці *Дополнительно* діалогового вікна *Свойства: Сервер печати* утиліта *Принтеры* з *Панели управления* встановлюються такі параметри сервера друку:

- *Вести журнал ошибок очереди печати*;
- *Вести журнал предупреждений очереди печати*;
- *Вести журнал сообщений очереди печати*.

3 Технічні відомості про систему ЛОЗА-1

3.1 Склад та розміщення програмного забезпечення системи

Після інсталяції програмні засоби системи ЛОЗА-1 розміщуються в окремій папці жорсткого диска, яка в цьому документі позначається %LOZA%. Склад програмного забезпечення системи, його розміщення в папці та її підпапках наведені в таблиці 3.1.

Таблиця 3.1 – Розміщення програмного забезпечення системи

Папка	Призначення або вміст
%LOZA%	коренева папка
DOC	коренева папка для збереження текстових документів
Help	коренева папка для файлів довідки
ProDoc	файли довідки для програми <i>Захищені документи</i>
Lib	програма <i>Настройка та відновлення</i> , спільні бібліотеки (*.dll, ...) та утиліти
Programs	коренева папка для клієнтських програм
ProDoc	програма <i>Захищені документи</i> (ProDoc.exe)
Security	коренева папка для ПЗ захисту інформації
Help	файли довідки адміністративних утиліт
Log	файли звітів перевірок цілісності
Backup	резервні копії журналів
Report	звіти про помилки та небезпечні події
SecLog	журнал захисту
Programs	адміністративні утиліти: – <i>Монітор захисту</i> (secmon.exe); – <i>Керування захистом</i> (safety.exe); – <i>Аудитор</i> (auditor.exe)
Safety	база даних захисту
Server	<i>Сервер безпеки</i> (lozasec.exe), <i>ЛОЗА Starter</i> (starter.exe), бібліотека LOZAGina.dll та деякі службові файли
SYSTEMP	тимчасові файли, необхідні для роботи системи

Під час інсталяції системи в папку %LOZA%\Lib записуються шаблон безпеки LOZA-1.inf (п. 2), а також спеціально розроблені утиліти WFolders, CDSPad та GetSID, призначені для службових цілей. Перша з них використовується для безповоротного видалення файлів вказаних папках, друга дозволяє переглянути та відкоригувати таблиці бази даних Safety, які мають спеціальний формат *.cds, а третя призначена для визначення SID користувача або групи користувачів у текстовому та шістнадцятковому вигляді. Ці утиліти мають простий інтуїтивний інтерфейс і не потребують окремих пояснень. Необхідність у використанні утиліт виникає лише під час встановлення або відновлення ПЗ системи.

3.2 Відновлення системи ЛОЗА-1

У виключних випадках після збоїв апаратного або програмного забезпечення засоби адміністрування, які входять до складу системи ЛОЗА-1, не дозволяють відновити її працездатність. У такій ситуації адміністратору необхідно застосувати програму *Відновлення системи ЛОЗА-1* (%LOZA%\LIB\LOZARecover.exe).

На рисунку 3.1 наведено головне вікно програми. Розташовані на ньому кнопки дозволяють виконати певні дії щодо відновлення системи. Всі ці дії виконуються автоматично під час інсталяції системи, тому виконання їх вручну необхідне тільки після серйозних збоїв.

Нижче докладно описано, що саме відбувається під час виконання кожної дії.

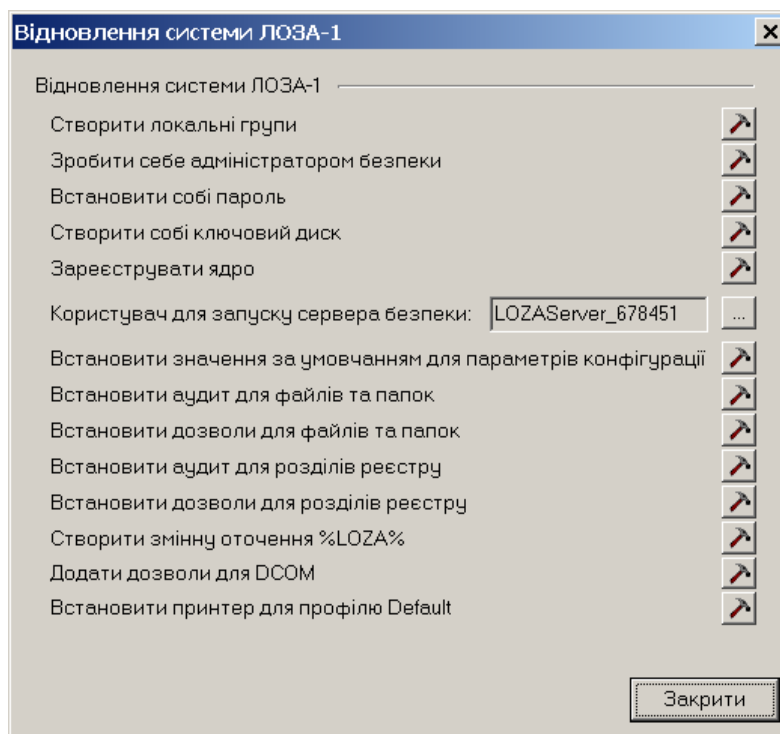


Рисунок 3.1

3.2.1 Створити локальні групи

Створюються локальні групи, необхідні для роботи системи ЛОЗА-1, і їм надаються певні права. Кожна група, крім групи *LOZAUers*, відповідає деякій ролі користувача або серверної програми. Перелік груп, ролей, що їм відповідають, та наданих їм прав наведений у таблиці 3.2.

Таблиця 3.2

Локальна група	Опис групи	Роль користувача	Права, що надаються групі
<i>LOZASecAdmins</i>	Адміністратори безпеки системи ЛОЗА-1	<i>Адміністратор безпеки</i>	Права не надаються
<i>LOZASysAdmins</i>	Системні адміністратори системи ЛОЗА-1	<i>Системний адміністратор</i>	Права не надаються
<i>LOZADocAdmins</i>	Адміністратори документів системи ЛОЗА-1	<i>Адміністратор документів</i>	Права не надаються

Локальна група	Опис групи	Роль користувача	Права, що надаються групі
<i>LOZAOrdinaryUsers</i>	Звичайні користувачі системи ЛОЗА-1	<i>Звичайний користувач</i>	Права не надаються
<i>LOZASecServers</i>	Сервери безпеки системи ЛОЗА-1	<i>Сервер безпеки</i>	Вход в качестве пакетного задания (Право входити у систему як пакетне завдання)
<i>LOZAUUsers</i>	Усі користувачі системи ЛОЗА-1		Права не надаються

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

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

3.2.2 Зробити себе адміністратором безпеки

Користувач, який виконує інсталяцію системи, стає адміністратором безпеки системи ЛОЗА-1.

Для цього дані про користувача заносяться до переліку користувачів системи ЛОЗА-1. Йому встановлюється роль *Адміністратор безпеки* та рівень доступу *Відкрита інформація*. Користувач також включається до груп *LOZASecAdmins* та *LOZAUUsers*.

3.2.3 Зареєструвати ядро

Ядро системи складають програми *LOZA Starter (starter.exe)* та *Сервер безпеки (lozasec.exe)*. Перша з них здійснює автоматичний запуск системи (а саме, програми *Сервер безпеки*) на початку роботи операційної системи. Вона розроблена як служба (service) ОС. Після інсталяції системи обидві програми знаходяться в папці *%LOZA%\Security\Server*.

Під час реєстрації ядра програма *Сервер безпеки* запускається з параметром */regserver*, а програма *LOZA Starter (starter.exe)* – із параметром */install*. Після реєстрації програма *LOZA Starter* буде сконфігурована таким чином:

- залежність від груп (DependOnGroup) – не залежить;
- залежність від служб (DependOnService) – залежить від служби *RpcSs*;
- ім'я (DisplayName) – *LOZA Starter*.
- обробка помилок (ErrorControl) – повідомляти про помилки (1);
- запуск від імені системи, тобто від імені облікового запису *СИСТЕМА* (ObjectName – *LocalSystem*);
- тип запуску (Start) – запуск під час старту операційної системи (2);
- тип служби (Type) – Win32-програма (0x10).

Необхідно вказати користувача, від імені якого запускатиметься *Сервер безпеки*. Цей користувач включається до груп *Адміністраторы*, *LOZASecServers* та *LOZAUUsers*, його пароль змінюється автоматично. Цей обліковий запис не можна використовувати жодному з “реальних” користувачів системи.

Перед проведенням деінсталяції ці програми дереєструються. Для цього вони запускаються з параметрами */unregserver* та */uninstall* відповідно.

3.2.4 Встановити значення за умовчанням для параметрів конфігурації

Для всіх параметрів конфігурації системи встановлюються значення за умовчанням.

3.2.5 Встановити аудит для файлів та папок

Для всіх папок, наведених у таблиці 3.1, та файлів, які в них знаходяться, встановлюється аудит відмов для всіх видів доступу, а також аудит успіхів для зміни дозволів і зміни власника.

Для папки *%LOZA%\SysTemp* встановлюється лише аудит успіхів для типів доступу *Смена разрешений* та *Смена владельца*, оскільки встановлення аудита відмов для інших видів доступу призводить до реєстрації великої кількості незначущих подій. З тієї ж причини для папки *%LOZA%\Programs* та її підпапок встановлюється лише аудит успіхів та відмов для типів доступу *Смена разрешений* та *Смена владельца*.

Відповідні установки наведені в таблиці 3.3.

Таблиця 3.3 –Аудит доступу до файлів та папок системи ЛОЗА-1

Папка	Група	Тип доступу	Тип аудита
%LOZA% та всі підпапки	Все	Усі види доступу	Отказ
		Смена разрешений Смена владельца	Успех; Отказ
%LOZA%\SysTemp	Все	Смена разрешений Смена владельца	Отказ
%LOZA%\Programs	Все	Смена разрешений Смена владельца	Успех; Отказ

3.2.6 Встановити дозволи для файлів та папок

Для всіх папок, наведених у таблиці 3.1, та файлів, які в них знаходяться, встановлюються дозволи на доступ згідно з таблицею 3.4. У цій таблиці не вказані підпапки, які успадковують дозволи від папок вищого рівня.

Використані в таблиці позначення наведені в переліку скорочень та позначень. У розшифровці дозволів у перших дужках вказано дозвіл для папок та підпапок, у других – дозвіл для файлів.

Таблиця 3.4 – Дозволи на доступ до папок системи ЛОЗА-1

Папка	Дозволи	
	Група	Дозволи для групи
%LOZA%	LOZASecAdmins LOZASecServers LOZAServers Администраторы СИСТЕМА	Изменение ¹ Изменение Список содержимого папки ² Изменение Изменение
DOC	LOZASecServers	Изменение

Папка		Дозволи		
		Група	Дозволи для групи	
	Help	LOZAUUsers	Изменение	
	Lib	LOZASecAdmins	Изменение	
		LOZASecServers	Изменение	
		LOZAUUsers	Чтение и выполнение	
		Администраторы	Чтение и выполнение	
		СИСТЕМА	Изменение	
	Programs	LOZASecAdmins	Изменение	
		LOZASecServers	Изменение	
		LOZAUUsers	Чтение и выполнение	
		СИСТЕМА	Изменение	
	Security	LOZASecAdmins	Изменение	
		LOZASecServers	Изменение	
		LOZASysAdmins	Изменение	
		СИСТЕМА	Изменение	
	Log	Backup	LOZASecAdmins	Изменение
			LOZASecServers	Изменение
			LOZASysAdmins	Чтение и выполнение
		Report	LOZASecAdmins	Изменение
			LOZASecServers	Изменение
		Seclog	LOZASecServers	Изменение
		Safety	LOZASecServers	Изменение
		Server	LOZASecAdmins	Изменение
			LOZASecServers	Изменение
			LOZASysAdmins	Изменение
			СИСТЕМА	Изменение
		SYSTEMP	LOZASecServers	Полный доступ

¹Изменение = (X R RA RE W A WA WE D RC) (X R RA RE W A WA WE D RC)

²Список содержимого папки = (X R RE RA RC) (Не указано)

3.2.7 Встановити аудит для розділів реєстру

Параметри конфігурації системи ЛОЗА-1 зберігаються в розділі реєстру HKEY_LOCAL_MACHINE\SOFTWARE\NПavtoprom\LOZA-1. Аудит доступу до цього розділу та всіх його підрозділів встановлюється відповідно до таблиці 3.5.

Таблиця 3.5 – Аудит доступу для розділу HKEY_LOCAL_MACHINE\SOFTWARE\NПavtoprom\LOZA-1

Група	Тип доступу	Тип аудита
Все	Запрос значения	Отказ
	Задание значения	Успех; Отказ
	Создание подраздела	Отказ
	Перечисление подразделов	Отказ
	Уведомление	Отказ
	Создание связи	Отказ
	Удаление	Успех; Отказ
	Запись DAC	Успех; Отказ
	Смена владельца	Успех; Отказ
	Чтение разрешений	Отказ

3.2.8 Встановити дозволи для розділів реєстру

Дозволи на доступ до розділу HKEY_LOCAL_MACHINE\SOFTWARE\NПavtoprom\LOZA-1 та всіх його підрозділів встановлюються відповідно до таблиці 3.6.

Таблиця 3.6 – Дозволи на доступ до розділу HKEY_LOCAL_MACHINE\SOFTWARE\NПavtoprom\LOZA-1

Група	Дозволи для групи
Администраторы LOZASecServers SYSTEM	Чтение Полный доступ Полный доступ

3.2.9 Створити змінну оточення %LOZA%

Створюється змінна оточення %LOZA%, яка вказує на кореневу папку системи LOZA-1.

3.2.10 Додати дозволи для DCOM

Встановлюється дозвіл на доступ до DCOM-серверів групі *Все*. Це необхідно для забезпечення можливості передачі COM-інтерфейсів зворотного виклику (нею користуються програма *Монітор захисту*). Переглянути та змінити встановлені для DCOM дозволи вручну можна за допомогою стандартної утиліти *dcomcnfg*, на сторінці *Безопасность по умолчанию*.

3.2.11 Встановити принтер для профілю Default

Для забезпечення можливості автоматичного друку звітів про роботу системи програмою *Сервер безпеки* (вона працює без інтерфейсу від імені службового користувача) необхідно внести відомості про встановлений за умовчанням принтер у системний профіль (профіль *Default*). Для цього програма *LOZATune* робить такі зміни в реєстр (наведені рекомендації запозичені зі статті Q152451 Microsoft Knowledge Base):

– копіює інформацію, що зберігається в розділі HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Devices (наприклад, параметр *HP LaserJet 5L* типу *REG_SZ* із значенням *winspool,LPT1:*) у розділ

HKEY_USERS.Default\Software\Microsoft\Windows NT\CurrentVersion\Devices (тобто створює параметр із тим самим іменем та типом і встановлює для нього таке ж значення);

– копіює інформацію, що зберігається у розділі *HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion*

PrinterPorts (наприклад, параметр *HP LaserJet 5L* типу *REG_SZ* із значенням *winspool,LPT1:,15,45*) у розділ

HKEY_USERS.Default\Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts;

– копіює інформацію, що зберігається у параметрі *Device* розділу *HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows* (наприклад,

HP LaserJet 5L,winspool,LPT1:) у параметр *Device* розділу *HKEY_USERS.Default\Software\Microsoft\Windows NT\CurrentVersion\Windows*.

Перелік скорочень та позначень

ОС операційна система
 ПЗ програмне забезпечення
 %LOZA% коренева папка системи ЛОЗА-1

Параметри конфігурації системи виділено рівномірним шрифтом.

Нижче наведені позначення видів доступу до файлів та папок.

Доступ	Позначення	Пояснення	
		Пояснення англійською	Пояснення українською
Execute	X	Execute a file or traverse a directory	Запуск файлу або перегляд папки
Read	R	Read file data or list directory entries	Читання вмісту файлів або папок
ReadAttr	RA	Read attributes	Читання атрибутів
ReadEa	RE	Read extended attributes	Читання додаткових атрибутів
Write	W	Write file data or create new file in directory	Запис у файл або створення файлу в папці
Append	A	Append data to a file or add subdirectory	Додавання даних у файл або створення підпапки <pre> var f1:TFormPrintPassw; begin {тадієї әеү òèðàæòááííý äîéóíáíò³â} f1:=TFormPrintPassw.Create(Application); TRY f1.ShowModal; FINALLY f1.Release; END;</pre>
WriteAttr	WA	Write attributes	Запис атрибутів
WriteEa	WE	Write extended attributes	Запис додаткових атрибутів
DeleteChild	DC	For a directory, delete entries in directory	Видалення файлу або підпапки з папки
Delete	D	Delete access	Видалення
ReadControl	RC	Read access to the owner, group, and discretionary access control list (ACL) of the security descriptor	Читання власника, групи або списку доступу (ACL) з дескриптора безпеки
WriteDac	WD	Write access to the owner, group, and discretionary access control list (ACL) of the security descriptor	Запис власника, групи або списку доступу (ACL) у дескриптор безпеки
takeOwnership	O	Write access to the owner	Запис власника