Товариство з обмеженою відповідальністю
Науково-дослідний інститут
«Автопром»

Система захисту інформації

ЛОЗА™-1

версія 4.3.0

ІНСТРУКЦІЯ СИСТЕМНОГО АДМІНІСТРАТОРА

ЛОЗА-1-4.І3.03.1

ТОВ НДІ “Автопром”
Київ, 2018

Зміст

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 (32-бітна версія);
- Microsoft Windows Vista, Service Pack 2 або вище (32- або 64-бітна версія);
- Microsoft Windows 7 (32- або 64-бітна версія);
- Microsoft Windows 8 (32- або 64-бітна версія);
- Microsoft Windows 8.1 (32- або 64-бітна версія);
- Microsoft Windows Server 2003 (32-бітна версія);
- Microsoft Windows Server 2008 (32- або 64-бітна версія);
- Microsoft Windows Server 2008 R2 (64-бітна версія).
- Microsoft Windows Server 2012 (64-бітна версія).
- Microsoft Windows Server 2012 R2 (64-бітна версія);
- Microsoft Windows Server 2016 (64-бітна версія);
- Microsoft Windows 10 (32- або 64-бітна версія).

Слід зазначити, що для коректної роботи системи з Windows 10 має бути встановлено кумулятивне оновлення KB3147461 або вище (можливий варіант, при якому операційна система буда раніше оновлена через інтернет).

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 2003;
- Microsoft Office 2007 (SP-2 або вище);
- Microsoft Office 2010;
- Microsoft Office 2013;
- Microsoft Office 2016.

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

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

2 Рекомендації з налаштування Windows

В операційних системах Windows 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 налаштувати Windows згідно із шаблоном *LOZA-1.inf*, достатньо запустити програму *Налаштування безпеки Windows (%LOZA%\LIB|LOZAWinSec.exe)* та натиснути кнопку *Налаштувати* (для застосування шаблона можна використати також стандартні засоби адміністрування Windows).

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

1) У секції [Privilege Rights] видалений рядок

sebatchlogonright =

(за наявності цього рядка під час застосування шаблона 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 шаблона *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 шаблона *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 налаштування 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 шаблона *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 паролі;
- 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, російського та українського алфавітів: A,B,C,D,…,Z, А, Б,…Я;
- строкові літери латинського, російського та українського алфавітів: a,b,c,d,…,z, а, б,…я;
- цифри: 0,1,2,3,…,9;
- спеціальні символи:

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

Для кожного новоствореного 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 аудиту

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

- Вход и выход (Аудит входа 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);
- Перезагрузка, 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 шаблона *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

Папкая				Призначення або вміст
%LOZA%				коренева папка
	DOC			коренева папка для збереження текстових документів
	Help			коренева папка для файлів довідки
		ProDoc		файли довідки для програми *Захищені документи*
	Lib			програма *Налаштування та відновлення*, спільні бібліотеки (*.dll, ...) та утиліти
	Programs			коренева папка для клієнтських програм
		ProDoc		програма *Захищені документи* (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: – *Монітор захисту* (secmon.exe); – *Керування захистом* (safety.exe); – *Аудитор* (auditor.exe)
		Safety		база даних захисту
		Server		*Сервер безпеки* (lozasec.exe), *LOZA Starter* (starter.exe), бібліотека LOZAGina.dll та деякі службові файли
	Servers			коренева папка для серверів клієнтських програм
		Doc		сервер документів LOZADocProcSrv.exe
	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 в указаних 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)*.

3.2.1 Відновлення

На рисунку 3.1 наведена сторінка *Відновлення* головного вікна програми. Розташовані на ній 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.

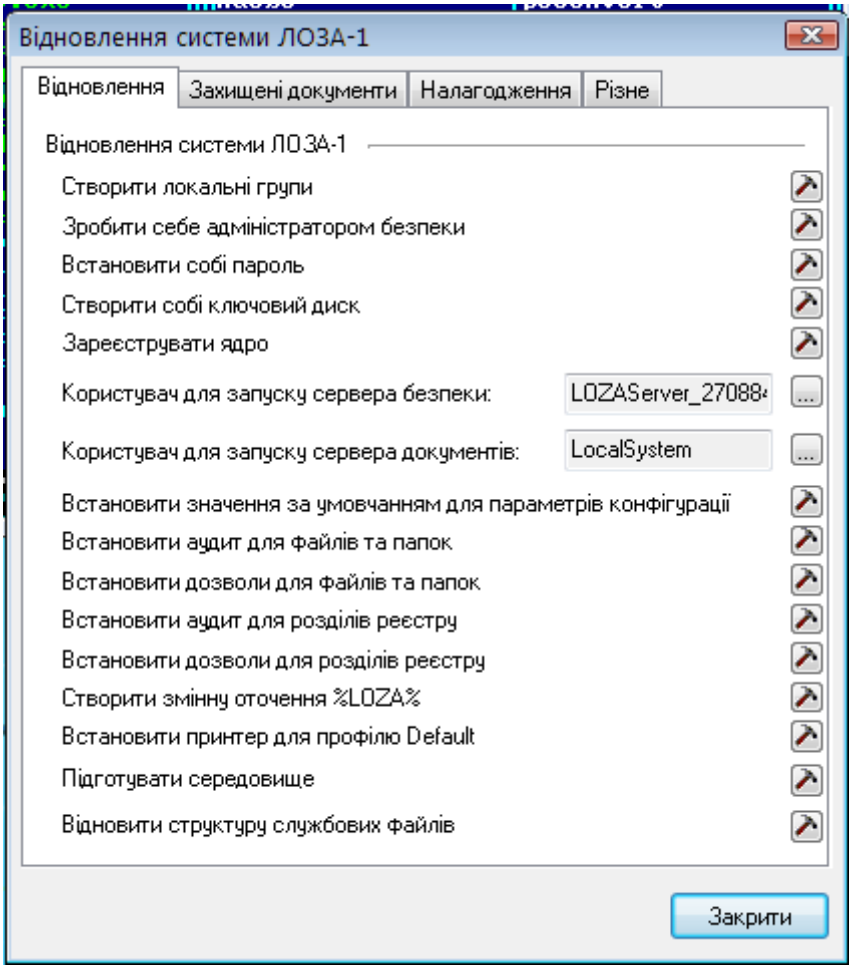

Рисунок 3.1

3.2.1.1 Створити локальні групи

Створюються локальні групи, необхідні для роботи системи ЛОЗА-1, і їм надаються певні права. Кожна група, крім групи *LOZAUsers*, 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
LOZASecAdmins	Адміністратори безпеки системи ЛОЗА-1	*Адміністратор безпеки*	Права не надаються
LOZASysAdmins	Системні адміністратори системи ЛОЗА-1	*Системний адміністратор*	Права не надаються
LOZADocAdmins	Адміністратори документів системи ЛОЗА-1	*Адміністратор документів*	Права не надаються
LOZAOrdinaryUsers	Звичайні користувачі системи ЛОЗА-1	*Звичайний користувач*	Права не надаються
LOZASecServers	Сервери безпеки системи ЛОЗА-1	*Сервер безпеки*	Вход в качестве пакетного задания (Право входити у систему як пакетне завдання)
LOZAUsers	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 ***Администраторы*** Windows. До групи ***Администраторы*** включається також службовий користувач, від імені якого запускається ***Сервер безпеки***.

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

3.2.1.2 Зробити себе адміністратором безпеки

Поточний користувач 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 *LOZAUsers*.

3.2.1.3 Створити собі ключовий диск

Для поточного користувача створюється ключовий диск, який обирається у відповідному діалозі.

3.2.1.4 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 знаходитимуться 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 *Администраторы*, *LOZASecServers* та *LOZAUsers*, 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.

3.2.1.5 Користувачі для запуску сервера безпеки та сервера документів

Тут зазначені «службові» користувачі, від імені яких запускається відповідний сервер. Після натискання трикрапки з'являється діалог, у якому можна обрати іншого користувача або підтвердити вибір того самого користувача. У разі вибору іншого користувача не слід обирати обліковий запис, який відповідає «реальним» користувачам системи. Можна набрати нове ім'я, відповідний користувач буде створений автоматично.

Цю дію необхідно виконати, якщо виникають проблеми із запуском відповідного сервера.

3.2.1.6 Встановити значення за умовчанням для параметрів конфігурації

Для всіх параметрів конфігурації системи встановлюються значення за умовчанням.

3.2.1.7 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 аудиту 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 аудиту
%LOZA% та всі підпапки	Все	Усі види доступу	Отказ
		Смена разрешений	Успех; Отказ

Папка	Група	Тип доступу	Тип аудиту
		Смена владельца	
%LOZA%\SysTemp	Все	Смена разрешений Смена владельца	Отказ
%LOZA%\Programs	Все	Смена разрешений Смена владельца	Успех; Отказ

3.2.1.8 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* *LOZAUsers* *Администраторы* *СИСТЕМА*	Изменение[1] Изменение Список содержимого папки[2] Изменение Изменение Изменение
	DOC			*LOZASecServers*	
	Help			*LOZAUsers*	Изменение
	Lib			*LOZASecAdmins*	Изменение
				LOZASecServers	Изменение
				LOZAUsers	Чтение и выполнение
				Администраторы	Чтение и выполнение
				СИСТЕМА	Изменение
	Programs			*LOZASecAdmins*	Изменение
				LOZASecServers	Изменение
				LOZAUsers	Чтение и выполнение
				СИСТЕМА	Изменение
	Security			*LOZASecAdmins*	Изменение
				LOZASecServers	Изменение
				LOZASysAdmins	Изменение
				СИСТЕМА	Изменение
		Log		*LOZASecAdmins*	Изменение
				LOZASecServers	Изменение
				LOZASysAdmins	Чтение и выполнение
			Backup	*LOZASecAdmins*	Изменение
				LOZASecServers	Изменение
			Report	*LOZASecAdmins*	Изменение
				LOZASecServers	Изменение
			Seclog	*LOZASecServers*	Изменение

Папка			Дозволи	
			Група	Дозволи для групи
		Safety	*LOZASecServers*	Изменение
		Server	*LOZASecAdmins*	Изменение
			LOZASecServers	Изменение
			LOZASysAdmins	Изменение
			СИСТЕМА	Изменение
	SYSTEMP		*LOZASecServers*	Полный доступ

[1]Изменение = (X R RA RE W A WA WE D RC) (X R RA RE W A WA WE D RC)
[2]Список содержимого папки = (X R RE RA RC) (Не указано)

3.2.1.9 Встановити аудит для розділів реєстру

Параметри конфігурації системи ЛОЗА-1 зберігаються в розділі реєстру HKEY_LOCAL_MACHINE\SOFTWARE\NIIavtoprom\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\ NIIavtoprom\LOZA-1

Група	Тип доступу	Тип аудиту
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

3.2.1.10 Встановити дозволи для розділів реєстру

Дозволи на доступ до розділу HKEY_LOCAL_MACHINE\SOFTWARE\NIIavtoprom\LOZA-1 встановлюються відповідно до таблиці 3.6.

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

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

3.2.1.11 Створити змінну оточення %LOZA%

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

3.2.1.12 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\WindowsNT\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*.

3.2.1.13 Підготувати середовище

Встановлюються значення параметрів реєстру, які забезпечують контроль входу до операційної системи з боку системи ЛОЗА-1.

У Windows XP/2003 відключається можливість запуску програм від імені іншого користувача, екран привітання та можливість швидкого переключення між користувачами. У інших версіях Windows відключається інструмент *Ножиці* (*Snipping tool*).

3.2.1.14 Відновити структуру службових файлів

Відновлюється коректна структура вибраних службових файлів. Для вибору файлів, структуру яких потрібно відновити, використовується діалогове вікно, наведене на рисунку 3.2.

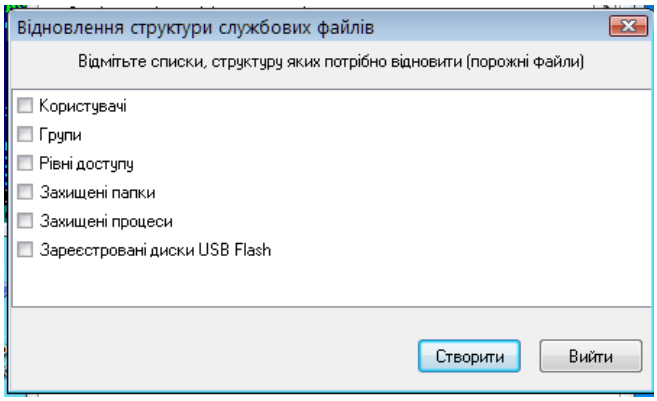

Рисунок 3.2

Цю дію можна виконати тільки у випадку, коли система знаходиться у стані відновлення.

Слід зазначити, що після відновлення файл буде порожній. Тому рекомендується періодично робити експорт службових файлів, щоб можна було відновити їх вміст шляхом імпорту. Якщо відновлюється структура списку користувачів системи ЛОЗА. То необхідно виконати ще одну дію, а саме – зробити себе адміністратором безпеки. В іншому випадку система ЛОЗА не матиме жодного користувача для свого функціонування.

3.2.2 Захищені документи

На рисунку 3.3 наведена сторінка *Захищені документи* головного вікна програми.

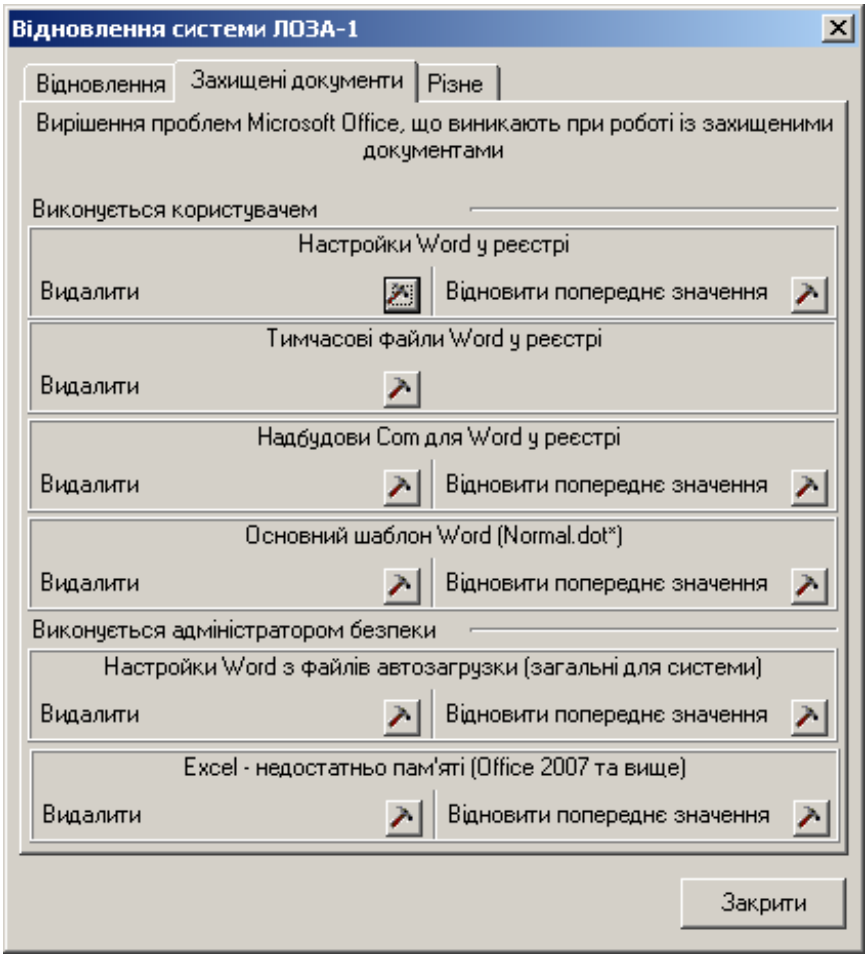

Рисунок 3.3

Нижче докладно описано, що саме відбувається під час виконання кожної дії. При цьому слід пам’ятати, що більшість проблем пов’язана із можливими конфліктами у налаштуваннях або некоректним встановленням самого Microsoft Office. Використання програм MS Office у контейнері (як передбачено у програмі *Захищені документи*) потребує дуже обережного поводження з налаштуваннями Word та Excel.

3.2.2.1 Налаштування Word у реєстрі

При натисканні кнопки *Видалити* відбувається перейменування ключів реєстру:

– *HKEY_CURRENT_USER\Software\Microsoft\Office\<**версія** MS Office>\Word\Data* та

– *HKEY_CURRENT_USER\Software\Microsoft\Office\<**версія** MS Office>\Word\Options*

у

– *HKEY_CURRENT_USER\Software\Microsoft\Office\<**версія** MS Office>\Word\LozaBackUpData* та

– *HKEY_CURRENT_USER\Software\Microsoft\Office\<**версія** MS Office>\Word\LozaBackUpOptions.*

Відповідно Word замість налаштувань, які зберігались у цих розділах, застосує передбачені за умовчанням.

При натисканні кнопки ***Відновити попереднє значення*** відбувається зворотне перейменування ключів реєстру (якщо раніше були створені копії цих ключів, тобто виконувалась процедура ***Видалити***).

Вказані ключі можуть містити налаштування, що конфліктують з використанням MS Word у контейнері (що передбачено програмою ***Захищені документи***), тому їх вилучення може виправити ситуацію.

3.2.2.2 Тимчасові файли Word у реєстрі

При натисканні кнопки ***Видалити*** відбувається видалення з реєстру значень, що можуть містити посилання на відсутні або недоступні директорії. Передбачено лише видалення відповідних значень (без подальшого відновлення).

Ці значення наведені у таблиці 3.7.

Таблиця 3.7 – Дані про тимчасові файли, що використовує Word, у реєстрі

Розділ	Значення
HKEY_CURRENT_USER\Software\Microsoft\Office\ <версія MS Office>\Word\Options	AUTOSAVE-PATH
HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\Shell Folders	Cache
HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\ User Shell Folders	Cache

3.2.2.3 Надбудови Com для Word у реєстрі

При натисканні кнопки ***Видалити*** відбувається перейменування ключа реєстру:
HKEY_CURRENT_USER\Software\Microsoft\Office\Word\Addins

у

HKEY_CURRENT_USER\Software\Microsoft\Office\Word\LozaBackUpAddins

Відповідно Word не буде використовувати надбудови. Надбудови можна відключити також у самому Word.

При натисканні кнопки ***Відновити попереднє значення*** відбувається зворотне перейменування ключа реєстру (якщо раніше виконувалась процедура ***Видалити***).

3.2.2.4 Основний шаблон Word (Normal)

При натисканні кнопки ***Видалити*** відбувається перейменування основного шаблону MS Word (Normal.dot або Normal.dotm в залежності від версії MS Office) у Normal.dot(m).Lbk. А MS Word при старті створює шаблон, що передбачений за умовчанням. Розташування шаблону залежить від версії Windows. При натисканні

кнопки *Відновити попереднє значення* відбувається зворотне перейменування файлу (якщо раніше виконувалась процедура *Видалити*).

3.2.2.5 Налаштування Word з файлів автозагрузки (загальні для системи)

Ця функція доступна тільки користувачеві з правами адміністратора і є загальною для системи.

При натисканні кнопки *Видалити* відбувається перейменування файлів, що містяться у папці автозагрузки Word, у файли з розширенням .Lbk. Ці файли Word не використовує, але в подальшому вони можуть отримати попередні імена і знову використовуватись як шаблони Word.

3.2.2.6 Excel - недостатньо пам'яті (Office 2007 та вище)

Проблему з використанням пам'яті в Excel може вирішити видалення (перед цим відбувається експорт в файл для подальшого відновлення) розділу реєстру:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Installer\UserData\<SID конкретного користувача> \Components\ AD95649F068525549B26938D7D18FEA7

для кожного користувача Windows.

Відновлення відбувається з файлів, що були зроблені раніше для окремих користувачів.

3.2.3 Різне

На рисунку 3.4 наведена сторінка *Різне* головного вікна програми.

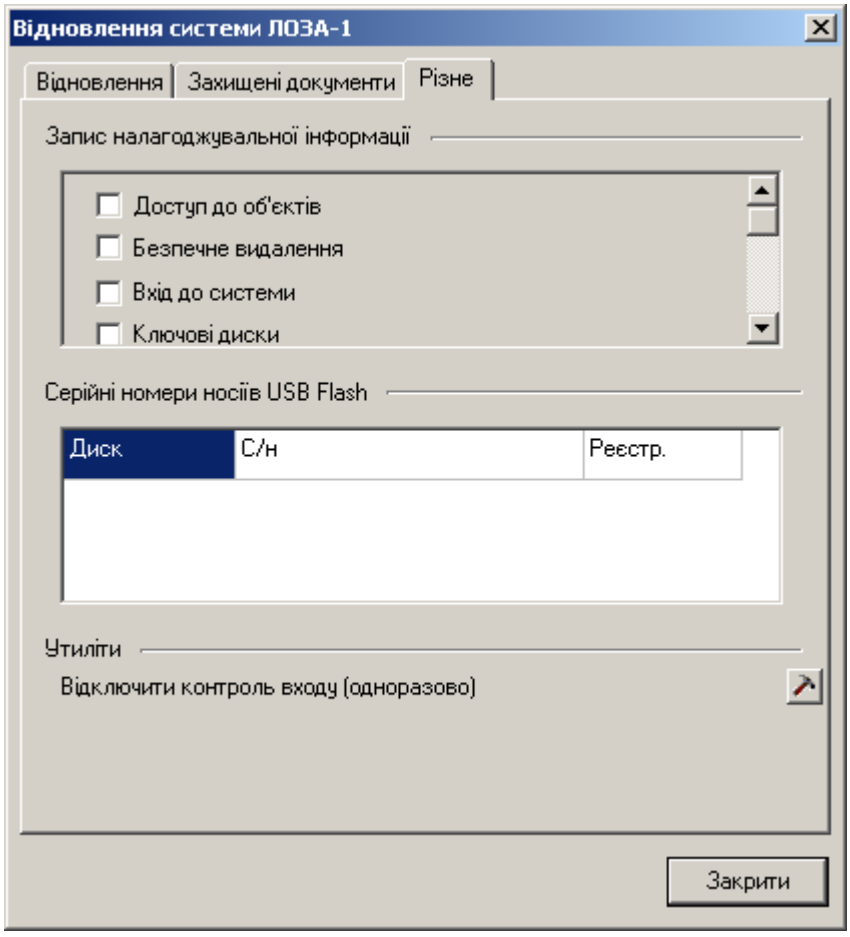

Рисунок 3.4

3.2.3.1 Запис налагоджувальної інформації

Відмітка пунктів в групі *Запис налагоджувальної інформації означає,* що відповідна інформація буде записуватись у текстовий файл, розташований в папці C:\. Ім’я файлу залежить від компоненти, яка здійснює запис. Використовуються такі імена: LOZASec.txt, LOZALgf.txt, LOZAFilterMgr.txt та ін. Для цих файлів встановлений граничний розмір (орієнтовно – 500КБ), по досягненні цього розміру попередній файл не видаляється, а перейменовується у файл *.tx1.

3.2.3.2 Серійні номери носіїв USB Flash

Інколи у користувачів системи ЛОЗА-1 виникає необхідність відновити реєстраційний носій USB Flash. Для цього слід повідомити розробникам серійний номер носія. Це можна зробити за допомогою стандартних засобів Windows, а можна також скористуватись наведеним на сторінці *Різне* переліком встановлених дисків з їхніми серійними номерами (див. рис. 3.5). У цьому ж переліку вказано, чи є диск реєстраційним носієм системи ЛОЗА-1.

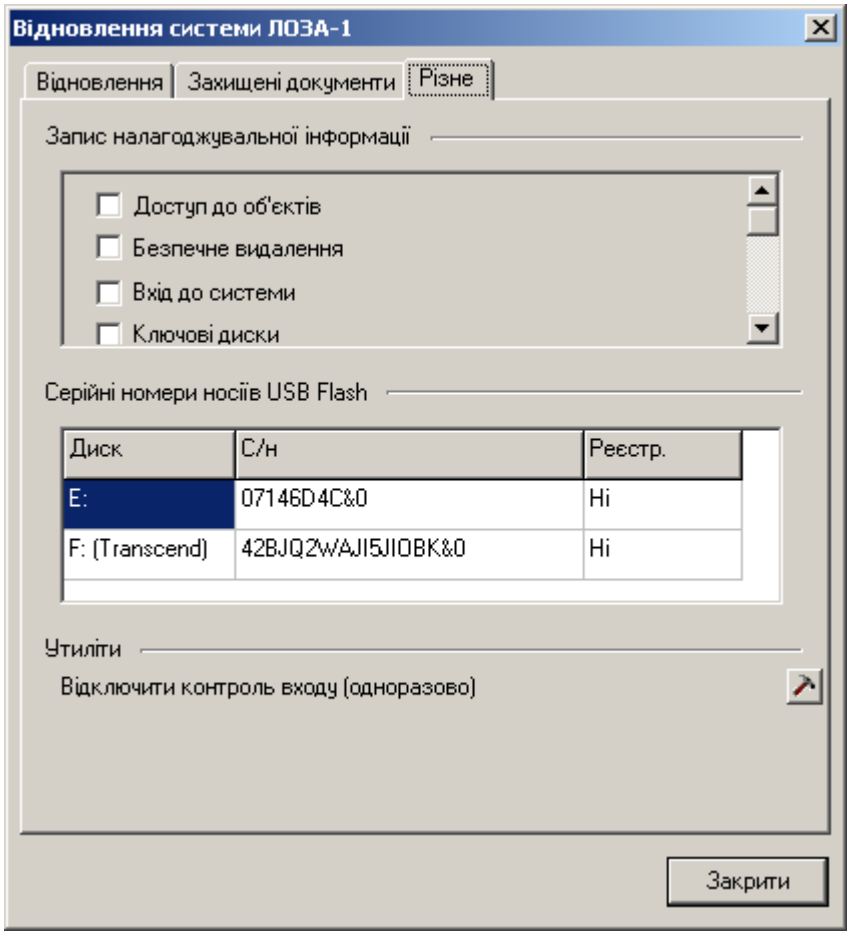

Рисунок 3.5

3.2.3.3 Відключити контроль входу (одноразово)

У деяких випадках виникає необхідність відключення контролю входу до операційної системи з боку системи ЛОЗА-1. Це відключення діє тільки до першого перезавантаження ОС.

Для Windows XP/2003 відключення контролю означає видалення параметра реєстру GinaDLL у розділі HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

Для Windows Vista/7/8/10/2012/2016 видаляються такі розділи реєстру:

– HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{9D5790A3-2401-4193-8392-2587C8C76472}

– HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{9D5790A3-2401-4193-8392-2587C8C76472}.

3.3 Засоби автоматизації

Система ЛОЗА-1 містить засоби автоматизації, які можуть бути використані, наприклад, для вирішення таких завдань:

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

Автоматизація полягає у виконанні перелічених в таблиці 3.1 команд. Кожна команда характеризується такими параметрами:

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

Таблиця 3.1

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

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

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

3.4 Автоматизація процесу встановлення системи

Файл, який здійснює інсталяцію системи LOZA-1_Setup.exe (LOZA-1_HS_Setup.exe – для конфігурації „Підвищена безпека”) може приймати параметри командного рядка, наведені в таблиці 3.2. Останні три параметри є стандартними для файлів інсталяції, створених за допомогою Inno Setup.

Таблиця 3.2

Параметр	Пояснення
ResponceFile=<file_name>	file_name – ім’я файлу, який містить параметри початкових налаштувань системи. Докладно вони описані нижче
AddProtectedFolders	Під час встановлення додаються захищені папки, вказані в файлі, що заданий в параметрі ResponceFile. Параметр докладно описаний нижче
/DIR="x:\dirname"	Папка, в яку буде запропоновано встановити систему. За умовчанням – %ProgramFiles%\LOZA-1
/SILENT	Не виводити діалоги майстра інсталяції
/VERYSILENT	Те ж саме, що й /SILENT і, додатково, означає не виводити індикатор прогресу установки

Параметр ResponceFile=<file_name> дозволяє автоматизувати встановлення значень для параметрів роботи системи, яке виконується під час початкових налаштувань, наприкінці процесу встановлення. Файл file_name має структуру ini-файла Windows, тобто містить секції та параметри. Він може містити такі дані:

– початкові значення для параметрів конфігурації (назви секцій, параметрів та можливих значень параметрів конфігурації наведені в Додатку А до документа "Загальний опис системи");

– значення, які встановлюються під час початкових налаштувань системи (секція *InitialTune*);

– перелік захищених папок, які будуть додані під час установки системи (секція *ProtectedFolders*).

Параметри секції *InitialTune* описані в таблиці 3.3.

Таблиця 3.3 – параметри секції InitialTune

Параметр	Пояснення	Можливі значення	Примітка
ShowAdminSecLevelDialog	Визначає, чи виводити діалог встановлення рівня допуску адміністратора безпеки	0 – Ні 1 – Так	
AdminSecLevel	Значення для рівня допуску адміністратора безпеки. Використовується тільки у випадку ShowAdminSecLevelDialog=0	20- ЦТ 30 – Т 60 – ДСК 70 – конфіденційно 90 – відкрита інформація	Значення за умовчанням – 90
ShowAdminPasswordDialog	Визначає, чи виводити діалог встановлення пароля адміністратора безпеки	0 – Ні 1 – Так	
AdminPassword	Пароль адміністратора безпеки Використовується тільки у випадку ShowAdminPasswordDialog =0		

Параметр	Пояснення	Можливі значення	Примітка
ShowMaxDocSecrecyLevelDialog	Визначає, чи виводити діалог встановлення максимального рівня доступу	0 – Ні 1 – Так	
MaxDocSecLevel	Значення для максимального рівня доступу. Використовується тільки у випадку ShowMaxDocSecrecyLevelDialog=0	20- ЦТ 30 – Т 60 – ДСК 70 – конфіденційно 90 – відкрита інформація	
ShowLogonParsDialog	Визначає, чи виводити діалог встановлення параметрів входу до системи	0 – Ні 1 – Так	Значення можна встановити окремо для кожного параметра конфігурації
ShowDisksForDocumentsDialog	Визначає, чи виводити діалог визначення дисків для зберігання документів	0 – Ні 1 – Так	Значення можна встановити окремо для кожного параметра конфігурації

Секція *ProtectedFolders* може містити один або декілька параметрів, які іменуються за шаблоном *ProtectedFolder1, ProtectedFolder2,…* Кожен з цих параметрів повинен містити текстовий рядок – представлення захищеної папки у форматі CommaText, наприклад:

```
ProtectedFolder1='"AccessList=""AccountSID=L-1-1-
0,ReadPermitted=1,WritePermitted=0,ReadDenied=0,WriteDenied=0""",SecLevel=9
0,SerialNumber=5&3A9wer0&0.1.0,RestrictProcesses=1,Processes=C:\Test.exe*$7
5BAB9E6,Path=C:\Temp'
```

Серійний номер диска під час установки буде замінений на серійний номер диска на комп’ютері, на який встановлюється система.

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	Позна-чення	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
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