УДК 004.4.5, 681.030

АВТОМАТИЧНЕ НАЛАШТУВАННЯ І ПЕРЕВІРКА НАЛАШТУВАНЬ СЛУЖБ ОПЕРАЦІЙНОЇ СИСТЕМИ ПРИ ВИКОРИСТАННІ КОМПЛЕКСНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Денис Танцюра
НДЦ "ТЕЗІС" НТУУ "КПІ"

Анотація: **Запропоновано і розроблено різні варіанти налаштування і перевірки налаштувань служб операційної системи штатними засобами, при використанні різних комплексів засобів захисту інформації в автоматизованих системах класу 1. Проведено досліди шодо можливості застосування запропонованих і розроблених варіантів автоматичного налаштування для автоматизованих систем з різними комплексами засобів захисту**.

Summary: **The proposed and developed different variants customization and check the settings of the operating system services by regular means, using different complexes of information security in automated systems Class 1. Conducted experiments are unambiguous applicability of the proposed and developed variants for automatic configuration of automated systems with different complexes protection means.**

Ключові слова: **Комплексна система захисту інформації (КСЗІ), комплекс засобів захисту (КЗЗ), автоматичне налаштування служб операційної системи (ОС), шаблон безпеки, консольні команди, bat-файл**.

І Вступ

При створенні комплексних систем захисту інформації в автоматизованих системах (АС) зазвичай використовують перевірені та надійні засоби – ті що мають експертні висновки. Особливої уваги заслуговує АС класу 1, яка представляє собою одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності, відповідно до НД ТЗІ 2.5-005 -99 [1], тобто окремий комп'ютер без мережевих з'єднань. Так у нашій державі для створення КСЗІ в АС класу 1 використовують частіше за все наступні засоби [2]: Гриф, Рубіж-РСО, Лоза. Хоча ОС Windows 7 теж має експертний висновок, але не має необхідних опублікованих відомостей (експертних рекомендацій) щодо її налаштування. Так, навіть при використанні цих засобів, все одно виникає потреба у налаштуванні певних служб ОС [3], а при експертизі КСЗІ – перевірці цих налаштувань. Зазвичай, іноді при створенні і майже завжди при експертизі КСЗІ – необхідно виконати великий обсяг робіт за малий час, тому виникає потреба знаходження швидких, надійних та зручних практичних реалізацій усіх частин робіт, адже від їх повного виконання залежить і якість функціонування КСЗІ, тобто захисту інформації. А через обмеження часу та значної кількості служб виникає проблема швидкого та надійного налаштування та перевірки цих налаштувань, як при створенні КСЗІ, так і під час первинної або чергової експертизи. Використання іншого – спеціалізованого програмного забезпечення, спрямованого на такі функції – має також свої особливості і обмеження, наприклад, обмеження автоматичного налаштування не всіх, а частини служб, без зміни налаштувань інших, або відсутність експертного висновку. Також використання іншого – спеціалізованого програмного забезпечення (ПЗ) [4] чи спеціально розроблених шаблонів безпеки [5] – може обмежуватися самим засобом захисту, який при певному налаштуванні може його блокувати, а переналаштовувати його не завжди є можливість.

Також при використанні різних ОС : Windows XP, Windows Vista, Windows 7, їх повноти та сервіс-паків оновлення – перелік необхідних та рекомендованих до налаштувань служб ОС [3, 6] відрізняється за назвами, наявністю (може взагалі не бути) та присутністю (за відсутності можуть бути встановлені) служб ОС [7 – 10].

Окрім стороннього програмного забезпечення немає нічого іншого, як використання штатних засобів самої операційної системи. Так, основний спосіб налаштування служб операційної системи – це використання оснастки serveices.msc [11 – 13]. За допомогою неї, у разі відсутності обмежень до неї засобом захисту можна налаштувати необхідні служби у ручному режимі. Але це не зовсім зручно і може зайняти тривалий час. Враховуючи існування різних локалізацій ОС Windows деякі служби можуть мати оригінальну назву (без перекладу), або мати трохи інші назви [13 – 15], що ускладнює пошук і їх налаштування. Для швидкого та надійного налаштування залишається два шляхи: використання шаблонів безпеки [16] (що, правда, може бути теж обмежене засобом захисту) і адміністративних інструментів – bat-файлів [17, 18] для налаштування і перевірки налаштувань служб ОС.

Шаблони безпеки – звичайний текстовий файл з розширенням inf, що представляє конфігурацію безпеки або політику безпеки. Шаблони безпеки застосовуваються до політики локального комп'ютера або імпортуються в об'єкт групової політики [19 – 21].

Використання bat-файлів – найбільш швидкий, простий і зручний спосіб автоматизації дій користувача за допомогою використання спеціально розроблених сценаріїв. Вони використовуються зазвичай для швидкого створення скриптів, візуалізації виконуваних дій при виконанні сценарію, відображення результатів роботи скрипту на екрані, інформування про завершення роботи скрипту, виконання зовнішніх програм під час роботи скрипту.

Отже, необхідно розробити спосіб швидкого, надійного та зручного налаштування і перевірки необхідних служб ОС відповідно до вимог функціонування АС класу 1 [3, 6] штатними засобами ОС – розробити шаблон безпеки і як його альтернатива – bat-файл. Переконатися в можливості їх використання з різними КЗЗ.

II Розробка шаблону безпеки

У створенні шаблону безпеки немає нічого складного, особливо в тому випадку, коли треба налаштування тільки системних служб. Шаблон безпеки можна створити, знаючи його структуру і синтаксис, у звичайному текстовому файлі, зберігаючи його з розширенням inf. Або, простіше всього, можна його створити за допомогою компонента ОС – консолі управління Microsoft (mmc).

Можна навести приклад створення шаблону безпеки для ОС Windows XP.

Для використання консолі управління Microsoft достатньо натиснути на кнопку “Пуск”, у полі пошуку ввести mmc, а потім натиснути на кнопку “Enter”;

Відкриється порожня консоль ММС. У меню “Консоль” необхідно вибрати команду “Додати або видалити оснастку” або скористатися комбінацією клавіш Ctrl+M;

Натиснути на кнопку “Додати…” і у діалозі “Додавання та видалення оснасток” вибрати оснастку “Аналіз та налаштування безпеки” і натиснути на кнопку “Додати”; Так само необхідно додати і оснастку “Шаблони безпеки“. Потім натиснути – "Закрити".

У діалозі “Додавання або видалення оснасток” натиснути на кнопку “ОК”.

Далі у контекстному меню рядка C:\WINDOWS\security\templates обрати "Створити шаблон…" (Рис. 1). Далі у новому вікні ввести ім’я шаблону (SecServ) і його опис за необхідністю.

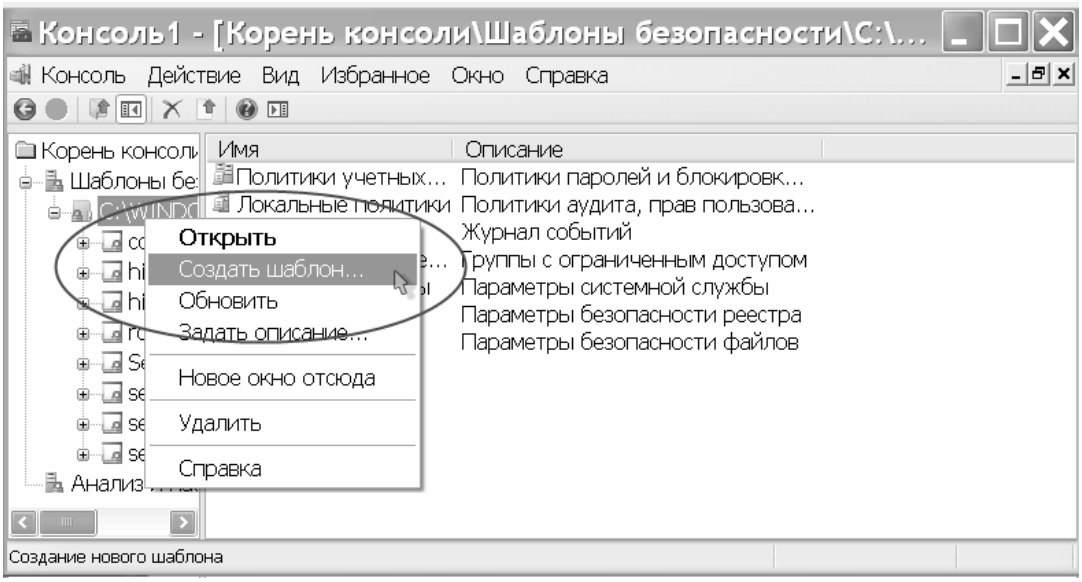

Рисунок 1 – Створення шаблону безпеки

Після цього можна обрати наш шаблон і обрати у ньому "Системні служби". Можна побачити перелік усіх можливих служб ОС з параметрами автозавантаження – "Не визначено". Потім у ручному режимі налаштувати необхідні служби, обов’язкові та рекомендовані до вимкнення [3], виставляючи у властивостях кожної служби відмітку про визначення параметру політики у шаблоні на – "Заборонено" (тобто заборонити

запуск служби). Також при необхідності можна налаштувати параметри безпеки для налаштування служби або погодитись з встановленими за замовченням. І натиснути кнопку “ОК”.

Наприклад, для КЗЗ Гриф обов’язковий перелік служб ОС Windows XP для вимкнення [3] наступний:

- DHCP-клієнт
- NetMeeting Remote Desktop Sharing
- Telnet
- Сервер (Server)
- Автоматичне оновлення (Автоматическое обновление)
- Бездротова настройка (Беспроводная конфигурация)
- Диспетчер авто-підключень віддаленого доступу (Диспетчер автоподключений удаленного доступа)
- Диспетчер підключень віддаленого доступу (Диспетчер подключений удаленного доступа)
- Маршрутизація та віддалений доступ (Маршрутизация и удаленный доступ)
- Брандмауер Windows/Загальний доступ до Інтернету (Общий доступ к подключению Интернет)
- Сервер каталогу обміну (Сервер папки обмена)
- Віддалений реєстр (Служба удаленного управления реестром).

Залежно від локалізації ОС назви цих служб можуть бути неідентичними. Також можливі варіанти, коли деяких служб може бути взагалі не встановлено, у такому разі Достатньо повного шаблону так просто не створити, адже налаштування таких служб буде невизначено і при переносі шаблону на іншу АС – налаштування таких служб не відбуватиметься.

Якщо відкрити тепер створений шаблон, то можна побачити його структуру і зміст (Рис. 2).

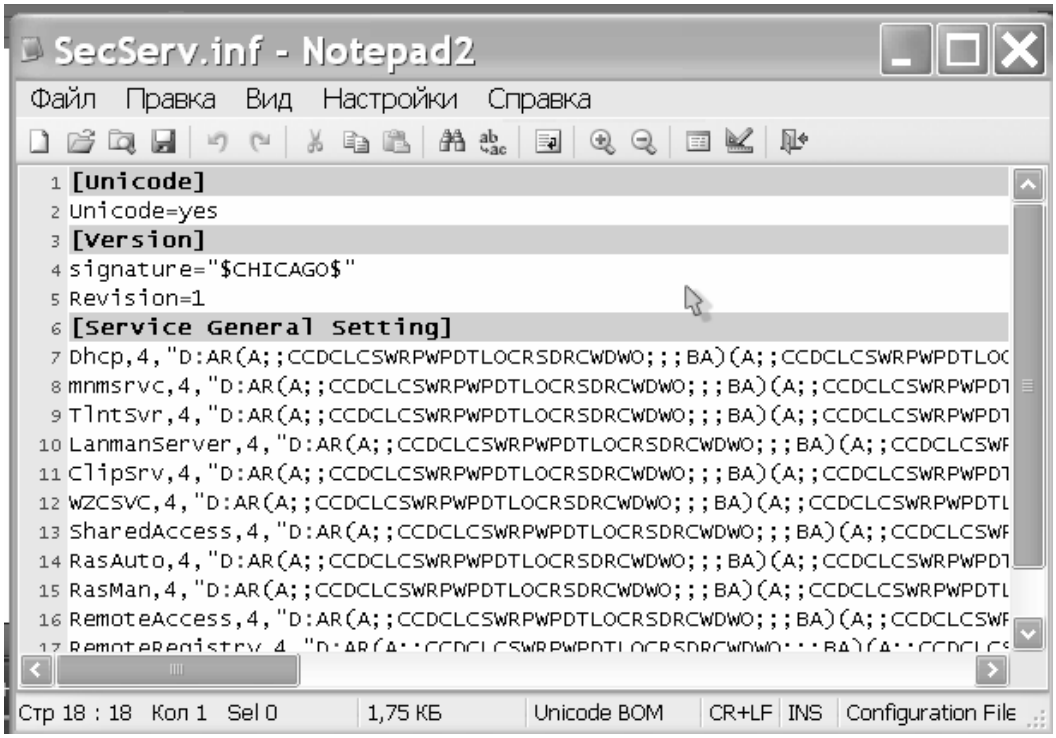

Рисунок 2 – Структура та зміст шаблону безпеки SecSrv.inf

Для перевірки, чи налаштовані служби ОС АС необхідним чином, потрібно у контекстному меню строки "Аналіз і налаштування безпеки" консолі керування обрати пункт "Відкрити базу даних…", після чого створити ім’я (наприклад DB1) і натиснути "Відкрити". Після цього обрати створений шаблон безпеки. Потім так само з контекстного меню строки "Аналіз і налаштування безпеки" консолі керування обрати пункт меню "Аналіз комп’ютера…". Після аналізу у вікні "Аналіз і налаштування безпеки" – "Системні служби" – можна побачити, чи відповідають налаштування служб необхідним. При правильних налаштуваннях служби – поряд з її назвою буде зелена галочка, інакше – червоний хрестик. При

необхідності швидкого налаштування потрібно у контекстному меню рядка "Аналіз і налаштування безпеки" консолі керування обрати пункт "Налаштувати комп'ютер…", після чого всі необхідні налаштування буде виконано згідно з вказаним шаблоном, при цьому буде збережено лог-файли виконаних дій – для відстеження помилок чи збоїв в процесі виконання налаштувань.

III Розробка БАТ-Файлу налаштування

Для створення bat-файлу необхідно знати і орієнтуватися у командах командної строки ОС [16,17]. Створити такий файл можна зі звичайного текстового файлу в блокноті ОС, зберігаючи його з розширенням bat. Налаштування системних служб ОС за допомогою командного файлу – через налаштування реєстру ОС або прямими командами налаштування служб, які самі автоматично налаштовують реєстр ОС.

Для відключення запуску певної служби можна скористатися наступною командою [18]:

```
sc config [ServiceName] start= disabled
```

де замість [ServiceName] вставляється системна назва відповідної служби. Системні назви служб – назви які прописані в реєстрі ОС у відповідному розділі
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\
їх можна також побачити в першому елементі параметрів строк у відповідному розділі налаштувань шаблона безпеки (Рис. 2.).

Таким чином, з додаванням записів результатів у текстовий файл, зміст bat-файлу буде наступним:

```
sc config ClipSrv start= disabled >> Log1.txt
sc config Dhcp start= disabled >> Log1.txt
sc config LanmanServer start= disabled >> Log1.txt
sc config mnmsrvc start= disabled >> Log1.txt
sc config RasAuto start= disabled >> Log1.txt
sc config RasMan start= disabled >> Log1.txt
sc config RemoteAccess start= disabled >> Log1.txt
sc config RemoteRegistry start= disabled >> Log1.txt
sc config SharedAccess start= disabled >> Log1.txt
sc config TlntSvr start= disabled >> Log1.txt
sc config wuauserv start= disabled >> Log1.txt
sc config WZCSVC start= disabled >> Log1.txt
```

Також можна зразу й зупинити налаштовані служби, для чого до нашого файлу необхідно додати:

```
sc stop ClipSrv >> Log1.txt
sc stop Dhcp >> Log1.txt
sc stop LanmanServer >> Log1.txt
sc stop mnmsrvc >> Log1.txt
sc stop RasAuto >> Log1.txt
sc stop RasMan >> Log1.txt
sc stop RemoteAccess >> Log1.txt
sc stop RemoteRegistry >> Log1.txt
sc stop SharedAccess >> Log1.txt
sc stop TlntSvr >> Log1.txt
sc stop wuauserv >> Log1.txt
sc stop WZCSVC >> Log1.txt
```

Для того, щоб наш командний файл працював не тільки з системного диску, необхідно додати на початку файлу строку:

```
%SYSTEMDRIVE%
```

При спробах зупинити або запустити службу можуть виникати помилки [22 – 24]. Частіше за все помилки виникають через залежність дочірніх служб ОС і неможливість запустити відключені служби. Щоб не виникало помилок необхідно налаштовувати/зупиняти/запускати служби в певній послідовності, залежно від їх взаємозалежностей. Для кращого представлення залежностей служб ОС можна скористатися деревом залежностей служб ОС, яке можна скласти власноруч, перевіряючи залежність кожної служби, або скористатися автоматичним представленням дерева служб ОС вільнодоступними програмами [25] (Рис. 3.).

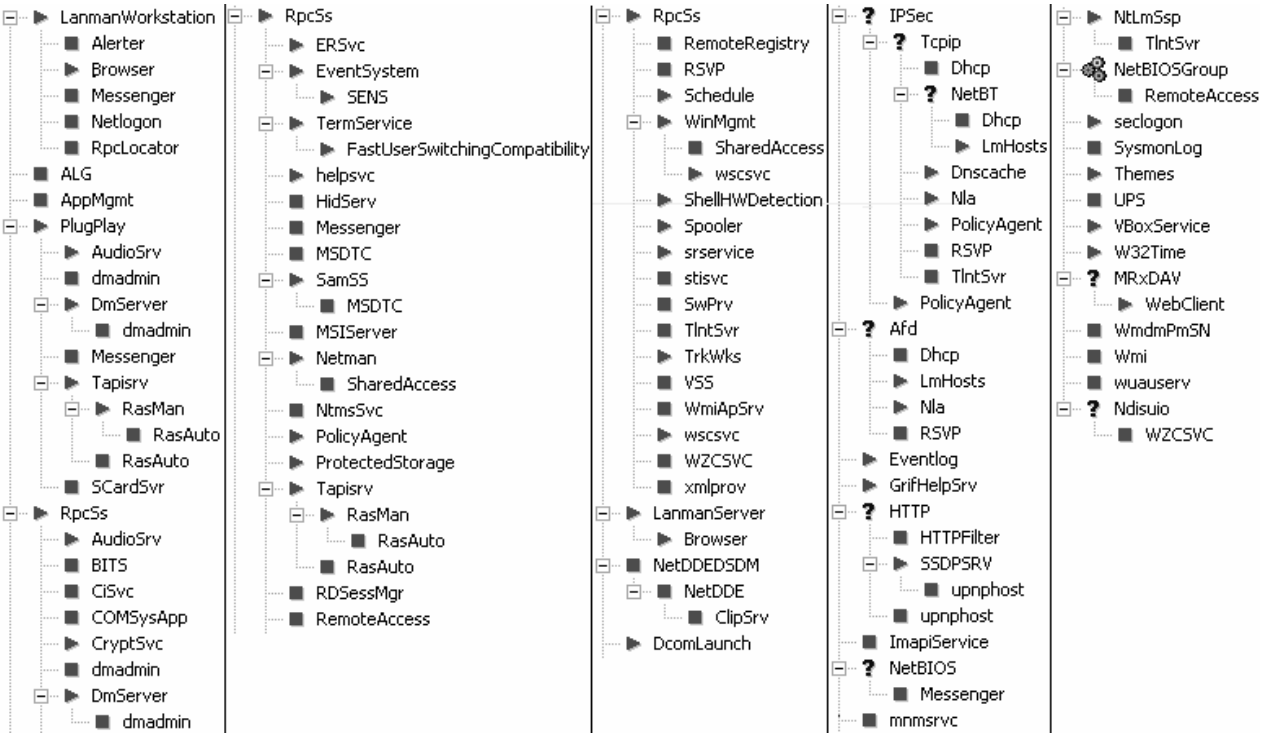

Рисунок 3 – Дерево залежностей служб ОС Windows XP (SP2 Pro)

Нажаль, для Windows 7 на даний момент немає у вільному доступі дерева залежностей служб ОС чи програм, які його відображають.

Як можна побачити від служби "Сервер" (lanmanserver) залежить служба "Оглядач комп'ютерів" (browser), тому перед зупиненням служби "Сервер" необхідно зупинити всі дочірні від неї служби, тобто в даному випадку в командному файлі необхідно перед командою вимкнення служби серверу додати наступну команду вимкнення:

```
sc stop browser
```

IV Розробка REG-Файлу налаштування

Налаштовувати служби можна і напряму через реєстр ОС, знаючи де і які параметри за що відповідають. Щоб не робити це вручну, можна скористатися зливанням додаткового файлу реєстру ОС, який являє собою звичайний текстовий файл, як і командний файл, тільки з розширенням reg, зі своєю синтаксисом та структурою. Зміст такого файлу у нашому випадку буде наступним:

```
Windows Registry Editor Version 5.00
; автоматичне вимкнення запуску необхідних служб Windows XP після встановлення
КЗЗ Гриф-3

; DHCP-клієнт
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\Dhcp]
"Start"=dword:00000004

; NetMeeting Remote Desktop Sharing
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\mnmsrvc]
"Start"=dword:00000004

; Telnet
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\TlntSvr]
"Start"=dword:00000004
```

```
; Сервер
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\lanmanserver]
"Start"=dword:00000004

; Автоматичне оновлення
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\wuauserv]
"Start"=dword:00000004

; Бездротова настройка
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\WZCSVC]
"Start"=dword:00000004

; Диспетчер авто-підключень віддаленого доступу
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RasAuto]
"Start"=dword:00000004

; Диспетчер підключень віддаленого доступу
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RasMan]
"Start"=dword:00000004

; Маршрутизація та віддалений доступ
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RemoteAccess]
"Start"=dword:00000004

;Брандмауэр Windows/Загальний доступ до Інтернету
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\SharedAccess]
"Start"=dword:00000004

; Сервер каталогу обміну
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\ClipSrv]
"Start"=dword:00000004

; Віддалений реєстр
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RemoteRegistry]
"Start"=dword:00000004
```

Для його застосування необхідно в контекстному меню обрати команду "Злиття" і погодитись. Для остаточного його застосування необхідно перезавантажити АС.

V Розробка БАТ-Файлу перевірки налаштувань

Тепер необхідно створити командний файл для перевірки налаштувань служб ОС, що буде дуже зручно при експертизі КСЗІ в АС класу 1.

Досить зручно виконувати перевірку правильності налаштувань служб ОС через реєстр. Для цього необхідно знати гілку реєстру служб ОС, назву параметру налаштування запуску і його значення.

Налаштування всіх служб у реєстрі операційної системи (Windows) знаходяться за шляхом "HKEY_LOCAL_MACHINE\system\currentcontrolset\services\".

У кожної служби параметр, який відповідає за її запуск, має назву "Start" і при необхідному налаштуванні, в даному випадку – заборона запуску, приймає значення "0x4", а при автоматичному, або ручному запуску – "0x2" і "0x3", відповідно.

Для запиту налаштувань реєстру можна скористуватися командою reg query., а для збереження звіту перевірки можна використати створюваний в процесі перевірки файл Zvit.txt. Таким чином для перевірки необхідних налаштувань служб ОС – командний файл буде мати наступний вигляд:

```
if not exist Zvit.txt echo Windows Registry Editor Version 5.00 > Zvit.txt

if "%1" == "" (goto exfun) else (goto exfun2)
:exfun
```

```
SETLOCAL ENABLEDELAYEDEXPANSION

Rem ; DHCP-клієнт
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\Dhcp ^
Start

Rem ; NetMeeting Remote Desktop Sharing
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\mnmsrvc ^
Start

Rem ; Telnet
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\TlntSvr ^
Start

Rem ; Сервер
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\lanmanserver ^
Start

Rem ; Автоматичне оновлення
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\wuauserv ^
Start

Rem ; Бездротове налаштування
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\WZCSVC ^
Start

Rem ; Диспетчер авто-підключень віддаленого доступу
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RasAuto ^
Start

Rem ; Диспетчер підключень віддаленого доступу
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RasMan ^
Start

Rem ; Маршрутизація та віддалений доступ
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RemoteAccess ^
Start

Rem ; Брандмауэр Windows/Загальний доступ до Інтернету
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\SharedAccess ^
Start

Rem ; Сервер каталогу обміну
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\ClipSrv ^
Start
```

```
Rem ; Віддалений реєстр
call Rego2012w7.bat ^
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RemoteRegistry ^
Start

echo ; Кількість правильно налаштованих служб (має бути 12): >> Zvit.txt
find /c "0x4" Zvit.txt >> Zvit.txt
echo ; >> Zvit.txt
echo ; Кількість не правильно налаштованих служб: >> Zvit.txt
find /c "0x3" Zvit.txt >> Zvit.txt
echo ; ma >> Zvit.txt
find /c "0x2" Zvit.txt >> Zvit.txt

goto exxit
:exfun2

set m1=%1
set m2=%2
reg query "!m1:#= !" /v !m2!

if %errorlevel%==0 (reg query "!m1:#= !" /v !m2! >> Zvit.txt
) else ( echo ; >> Zvit.txt
echo [!m1:#= !] >> Zvit.txt
echo ; Налаштування вказаної служби відсутні, може служба видалена з системи >>
Zvit.txt
)
)
:exxit
```

У результаті виконання цього файлу буде створений файл-звіт Zvit.txt, який буде містити необхідні параметри налаштування ОС АС та сповіщення про відповідність цих налаштувань заданим вимогам:

```
Windows Registry Editor Version 5.00

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\Dhcp
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\mnmsrvc
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\TlntSvr
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\lanmanserver
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0
```

```
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\wuauserv
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\WZCSVC
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RasAuto
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RasMan
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RemoteAccess
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\SharedAccess
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\ClipSrv
  Start REG_DWORD 0x4

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\RemoteRegistry
  Start REG_DWORD 0x4

; Кількість правильно налаштованих служб (має бути 12):

---------- ZVIT.TXT: 12
;
; Кількість не правильно налаштованих служб:

---------- ZVIT.TXT: 0
; ma

---------- ZVIT.TXT: 0
```

Швидкість виконання створених reg та bat файлів не перевищує кількох секундт і відразу дає представлення про правильність налаштування служб ОС АС відповідно до вимог.

Необхідно зазначити, що вимоги і рекомендації [3, 6] представлені тільки до ОС Windows XP, а для ОС Windows Vista та ОС Windows 7 необхідні уточнення, внаслідок відсутності, наявності і залежності деяких служб [7], та відсутності у вільному доступі експертних рекомендацій [2].

В результаті маємо:

- шаблон безпеки з налаштуваннят і перевірки служб ОС ОС Windows XP
- bat-файл для налаштування служб ОС

- reg-файл для налаштування служб ОС
- bat-файл для перевірки налаштувань служб ОС

VI Перевірка застосованості розроблених варіантів для різних КЗЗ

Тепер необхідно перевірити застосованість і роботу цих елементів для різних КЗЗ – Гриф версії 3, Рубіж-РСО, Лоза-1,та при використанні як КЗЗ самих ОС Windows XP, ОС Windows Vista, та ОС Windows 7. Автором була виконана перевірка застосованості запропонованих розроблених варіантів автоматичного налаштування і перевірка налаштувань служб ОС до різних варіантів КЗЗ. Результати перевірки наведені в табл. 1.

Таблиця 1 – Порівняння можливості застосування розроблених варіантів автоматичного налаштування служб ОС

Елементи перевірки \КЗЗ	Гриф версії 3 з ОС Windows XP	Рубіж-РСО (версії 2) з ОС Windows XP	Лоза-1 (версії 2) з ОС Windows XP	ОС Windows XP	ОС Windows Vista	ОС Windows 7
Автоматичне налаштування служб ОС	–	–	–	–	–	–
Використання стороннього ПЗ	Може бути обмежено налаштуванням	Може бути обмежено налаштуванням	+	+	+	+
Шаблон безпеки	–	+	+	+	+	+
Bat-файл для налаштування	+	+–	+	+	+	+
Reg-файл для налаштування	+	+	+	+	+	+
Bat-файл для перевірки	+	+–	+	+	+	+

VII Висновки

За результатами перевірки можна зробити висновки, що при використанні всіх вищенаведених варіантів не відбувається автоматичного налаштування служб ОС.

Для виконання швидкої, надійної та зручної перевірки та налаштування служб ОС відповідно до вимог АС класу 1 [3, 6] використання стороннього ПО може бути обмежено в деяких випадках, або взагалі неприпустимо (відповідно до вимог документації на КСЗІ у кожному конкретному випадку). Тому були запропоновані і розроблені різні варіанти, на основі відомих штатних засобів ОС. Також була виконана перевірка на застосовність цих варіантів при використанні різних КЗЗ для побудови КСЗІ в АС класу 1.

При використанні КЗЗ Гриф-3 (при повному налаштуванні) використання стороннього ПЗ буде обмежено. Також його використання обмежує застосування шаблонів безпеки, бо при встановленні і ініціалізації КЗЗ Гриф-3 видаляються необхідні оснастки з консолі керування ОС, що з іншого боку підвищує захист. Використання інших варіантів автоматичного налаштування служб під обліковим записом системного адміністратора не обмежене і працює коректно.

При використанні КЗЗ Рубіж-РСО застосування bat-файлів може бути ускладнене, бо час від часу деякі команди запізнюються і результат може бути не зовсім коректний. Але, враховуючи високу швидкодію розроблених bat-файлів, при кількаразовому послідовному виконанні bat-файлу – можна досягти коректних результатів.

При тестуванні на інших засобах – не було зафіксовано обмежень чи некоректних спрацювань розроблених варіантів автоматичного налаштування служб ОС.

В цілому використання запропонованих варіантів як альтернативи сторонньому ПО можна вважати придатним. Але внаслідок відсутності у відкритому доступі інформації щодо налаштувань відповідно до експертного висновку Windows 7 та відсутності рекомендацій налаштувань служб для ОС Windows 7 [3, 2] необхідно перевірити, проаналізувати і визначити той перлік служб ОС Windows 7, який потребує налаштувань відповідно до умов використання АС класу 1. Також було б корисним розробити шаблони налаштування ОС Windows 7, аналогічно вимогам ЕВ ОС Windows XP [6] та розробленим шаблонам [26] для спрощення побудови КСЗІ в АС класу 1 та АС класу 2.

Література: ***1.*** *НД ТЗІ 2.5-005 -99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (від " 28 " квітня 1999 р. № 22).* ***2.*** *Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України // Сайт Державної служби спеціального зв'язку та захисту інформації України (http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id= 78319&cat_id=39181).* ***3.*** *Комплекс средств защиты информации от несанкционированного доступа. «Гриф» версии 3. Руководство системного администратора. редакция 4. Киев 2012 – Институт компьютерных технологий, – 40 с. ил. (http:/www.ict.com.ua).* ***4.*** *SMART: A Utility For Tweaking Windows 7, Vista, XP Services Released. (http://www.thewindowsclub.com/smart-a-utility-for-tweaking-windows-7-vista-xp-services).* ***5.*** *Benchmarks > Os > Windows – Center for Internet Security Security Benchmarks Division (http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.os.windows).* ***6.****ЕКСПЕРТНИЙ ВИСНОВОК на Операційна система Microsoft® Windows® XP Professional з пакетом оновлення Service Pack 2. Сервіси безпеки. (msdb.com.ua/Downloads/Ukraine/Security/Expert/Expert_WXP.doc та http://www.microsoft.com/Ukraine/Security/Expert/Default.mspx).* ***7.*** *Default settings for services Windows XP Professional Product Documentation (http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sys_srv_default_settings.mspx?mfr=true).* ***8.*** *Service Configurations » Black Viper's Windows 7 Service Configurations (http://www.blackviper.com/windows-default-services/windows-7-default-services/).* ***9.*** *Ramesh Srinivasan | Windows 7 | 6th December 2010 (http://www.winhelponline.com/blog/windows-7-default-services-startup-config/).* ***10.*** *Windows 7 Default Services (http://social.technet.microsoft.com/wiki/contents/articles/4484.windows-7-default-services.aspx).* ***11.*** *Інформація з служби підтримки Microsoft (http://support.microsoft.com/kb/910337).* ***12.*** *Windows service (http://en.wikipedia.org/wiki/Windows_service).* ***13.*** *The Elder Geek sites – Services Guide for Windows XP (http://www.theeldergeek.com/services_guide.htm).* ***14.*** *Чеботарев Игорь – Описание служб в Windows NT/2000/XP (http://www.whatis.ru/reg/reg_w5.shtml).* ***15.*** *OSzone.netMicrosoftСлужбы WindowsСлужбы Windows XP Подробная информация по всем службам/ Опубликована: 17.02.2005 (http://www.oszone.net/2517/).* ***16.*** *Конференция iXBT.com » Программы: ОС и системное ПО » Можно создать для правки реестра *.reg файл для настройки служб в XP? (http://forum.ixbt.com/topic.cgi?id=22:74130).* ***17.*** *System Engineering – Сценарии для администрирования (Часть 1) (http://www.sysengineering.ru/Administration/ScriptsForAdministration01.aspx).* ***18.*** *Command-line reference A-Z (http://technet.microsoft.com/en-us/library/bb490890.aspx).* ***19.*** *Готовые шаблоны безопасности (http://technet.microsoft.com/ru-ru/library/cc787720(v=ws.10).aspx).* ***20.*** *Шаблоны безопасности (http://msdn.microsoft.com/ru-ru/library/bb521615(v=winembedded.51).aspx).* ***21.*** *Робота з оснащенням "Аналіз та налаштування безпеки", Windows, Операційні системи, статті. Автор: Vadim EasyCode Програмування, легко про складне ...(http://easy-code.com.ua/2012/08/robota-z-osnashhennyam-analiz-ta-nalashtuvannya-bezpeki-windows-operacijni-sistemi-statti/).* ***22.*** *System Error Codes (http://msdn.microsoft.com/en-us/library/windows/ desktop/ms681381(v=vs.85).aspx).* ***23.*** *Коды ошибок Windows (http://into.ucoz.ru/index/kody_oshibok_windows/0-17).* ***24.*** *Коды ошибок WINDOWS (http://www.shans-i.narod.ru/Disk_PC/Stat_PC/ Dop_MatPC/Stat_Dop_Mat/Stat_19.htm).* ***25.*** *WinServices 2.1.4.0 (http://www.softpedia.com/get/Tweak/System-Tweak/WinServices.shtml).* ***26.*** *Тодоренко Андрій, Танцюра Денис, Семенюк Сергій, Попелінов Олександр, Кліменко Євген., НДЦ "ТЕЗІС" НТУУ "КПІ". КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ КЛАСУ "1". Налаштування сервісів безпеки ОС MS Windows XP Pro SP2 за допомогою шаблону політики безпеки. ІАЛЦ.72.10.10.ХР.І4.01. Шаблон безпеки Windows XP Pro SP2 (SP3). Призначений для налаштовування сервісів безпеки операційної системи. Windows XP Pro SP2 (SP3) для автоматизованих систем класу "1".*