конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі – конфіденційна інформація);

інформація, що становить державну або іншу передбачену законом таємницю (далі – таємна інформація).

Важливість відкритої інформації визначається шляхом оцінки відповідних ризиків. Порядок та методика оцінки ризиків визначаються Державною службою спеціального зв'язку та захисту інформації України.

IV Висновки

Ширше бачення проблеми захисту інформації дозволяє більш активно та ефективно вирішувати її, перш за все, на концептуальному рівні. Держава повинна йти в ногу з розвитком сучасної науки. Саме внесення перспективних змін до законодавства України допоможе більш чітко визначитися з загальною концепцією побудови системи захисту інформації в державі, що в свою чергу сприятиме не тільки декларуванню необхідності вирішення проблеми захисту інформації, але й розв'язанню її по суті, що стає актуальним в умовах розвитку кібертероризму.

*Література: **1**. Общая парадигма защиты информации / П. И. Орлов, И. А. Громыко, В. В. Носов и др. // Защита информации. Конфидент. - 2003. - № 1(49).-С. 14 – 17. **2**. Носов В. В., Манжай А. В. Метод проектирования оптимальной системы защиты информации. // Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", Київ, 2004, вип. 9, с. 94 – 102 **3**. Капица Ю. Проблемы правовой охраны конфиденциальной информации в Украине (часть 2) // Інтелектуальна власність № 3, Київ, 2004, с. 27 – 33. **4**. Конституція України від 26. 06. 96 // Відомості Верховної Ради України, 1996, № 30 (23. 07. 96), ст. 141 **5**. Закон України «Про інформацію» від 02. 10. 92 // Відомості Верховної Ради України, 1992, № 48 (01. 12. 92), ст. 650 **6**. Закон України «Про державну таємницю» від 21. 01. 94 // Відомості Верховної Ради України, 1994, № 16 (19. 04. 94), ст. 93 **7**. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05. 07. 94 // Відомості Верховної Ради України, 1994, N 31 (02. 08. 94), ст. 286 **8**. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. Затверджена Постановою Кабінету міністрів України № 1893 від 27 листопада 1998 р. // Офіційний вісник України, 1998, № 48 (17. 12. 98), ст. 1764. **9**. «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Затверджені Постановою Кабінету міністрів України № 373 від 29 березня 2006 р. // Офіційний вісник України, 2006, № 13 (12. 04. 2006), ст. 878. **10**. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К. Г. Устименка) від 30 жовтня 1997 року // Офіційний вісник України, 1997, число 46 (02. 12. 97), №с. 126. **11.** «Концепція технічного захисту інформації в Україні». Затверджена Постановою Кабінету міністрів України № 1126 від 8 жовтня 1997 р.*

УДК 65.012.8:004.05

АВТОМАТИЗАЦІЯ КОНФІГУРАЦІЇ ПАРАМЕТРІВ БЕЗПЕКИ ОС MICROSOFT WINDOWS XP PROFESSIONAL SP2

Віталій Носов, Максим Кулік*, Олександр Манжай

*Харківський національний університет внутрішніх справ, *Науково-дослідний експертно-криміналістичний центр при УМВС України в м. Севастополі*

Анотація: **Наведено результати досліджень способів конфігурування параметрів безпеки ОС Microsoft Windows XP Professional SP2 та опис утиліти автоматизації конфігурування.**

Summary: **In the article are considered methods of configuration services security Microsoft Windows XP Professional SP2 and described utility for automation configuration.**

Ключові слова: **Інформаційна безпека, параметри безпеки операційної системи, Microsoft Windows XP Professional SP2, автоматизація конфігурації.**

I Вступ

В 2005 році Департамент спеціальних телекомунікаційних систем та захисту інформації Служби

безпеки України затвердив Експертний висновок [1], який засвідчує, що сервіси безпеки операційної системи Microsoft® Windows® XP Professional з пакетом оновлення Service Pack 2 і з пакетом підтримки української мови відповідає за рівнем гарантій Г-2 вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі „Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2. Технічні вимоги", сукупність яких визначається функціональним профілем КД-2, КО-1, КВ-2, ЦД-1, ЦО-1, ЦВ-2, ДР-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1, НА-1, НП-1. Допускається функціонування операційної системи в складі автоматизованих систем (АС) наступних класів [2]:

- „1" – одномашинний однокористувацький комплекс;
- „2" – локальний багатомашинний багатокористувацький комплекс (наприклад, локальна обчислювальна мережа);
- „3" – розподілений багатомашинний багатокористувацький комплекс з необхідністю передачі інформації через незахищене середовище.

АС класів 1 та 2 не передбачають доступу комп'ютерів до незахищеного середовища, зокрема, глобальної мережі Інтернет. Використання в послугах безпеки КВ-2, ЦВ-2, НВ-1, НА-1, НП-1 КД-2, ЦД-1 механізмів криптографічних перетворень для захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимоги щодо захисту якої встановлені законом, можливе лише за наявності документів, які засвідчують відповідність цих механізмів вимогам нормативно-правових актів з криптографічного захисту інформації.

Наданий Експертний висновок є правовою підставою для використання сервісів безпеки операційної системи Microsoft Windows XP Professional SP2 в автоматизованих системах державних органів, банківських установ і систем, що входять до складу довідково-пошукових ресурсів і містять несекретні дані або інформацію із грифом «Для службового користування».

В документі "Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2. Інсталяція об'єкта експертизи та конфігурування параметрів безпеки" викладено рекомендації щодо інсталяції та конфігурування параметрів безпеки операційної системи. Дослідження цих рекомендацій конфігурування параметрів безпеки операційної системи показало, що для практичного їх виконання і подальшої перевірки встановлених параметрів операційної системи необхідна автоматизація конфігурування параметрів безпеки ОС Microsoft Windows XP Professional SP2.

На кафедрі "Інформаційної безпеки" Харківського національного університету внутрішніх справ було досліджено способи конфігурування параметрів безпеки операційної системи та розроблено утиліту конфігурування параметрів безпеки ОС Microsoft Windows XP Professional SP2 згідно з вимогами документа "Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2. Інсталяція об'єкта експертизи та конфігурування параметрів безпеки". У статті приводяться результати досліджень і опис розробленої системи автоматизації конфігурування параметрів безпеки.

II Інструментарій керування безпекою ОС Microsoft Windows XP Professional

Згідно з [3] конфігурувати параметри безпеки треба за наступними розділами:

1. політика облікових записів;
2. параметри локальної політики;
3. журнал подій;
4. системні служби;
5. налаштування реєстру;
6. файлова система;
7. адміністративні шаблони ОС Windows XP;
8. політика обмеженого використання програм.

Для оцінки практичного застосування рекомендацій із конфігурування параметрів безпеки необхідно оцінити наявний інструментарій керування безпекою ОС Microsoft Windows XP Professional. Інструментами, що мають безпосереднє відношення до безпеки в ОС Microsoft Windows XP Professional, є:

- *комплект інструментів для аналізу й налаштування безпеки;*
- *оснащення Group Policy (Групова політика);*
- *інструмент налаштування Політики обмеженого використання програм.*

Дамо цим інструментам коротку характеристику. До складу *комплекту інструментів аналізу й налаштування безпеки* входять:

- Security Templates (Шаблони безпеки);

- Security Configuration and Analysis (Аналіз і налаштування безпеки);
- утиліта secedit (а також команда gpupdate, що замінила застарілий параметр /refreshpolicy).

Два із цих компонентів – Security Templates (Шаблони безпеки) і Security Configuration and Analysis (Аналіз і налаштування безпеки) виконані у вигляді оснащень (snap-in) консолі керування Microsoft Management Console (MMC). Ці компоненти дають можливість настроювати й аналізувати систему безпеки Microsoft Windows XP Professional, а також здійснювати її аудит. Третій компонент, представлений утилітою командного рядка secedit, дозволяє настроювати і аналізувати параметри системи безпеки.

Оснащення Group Policy дозволяє глобально застосувати заздалегідь налаштовані політики безпеки відразу на всіх комп'ютерах локальної мережі. Групова політика являє собою набір політик, які торкаються конфігурації користувача й комп'ютера, а також параметри безпеки, визначені в шаблонах безпеки. Налаштована політика називається об'єктом групової політики (GPO – Group Policy Object). Такий об'єкт можливо створити, а потім застосувати до контейнерів групової політики (GPC – Group Policy Container). Контейнери GPC, у свою чергу, є об'єктами Active Directory (ADO – Active Directory Objects), на які поширюється дія групової політики. Об'єктами групової політики можливо маніпулювати за допомогою: Group Policy Editor (Редактор групової політики) та оснащення Group Policy MMC.

Інструмент налаштування Політики обмеженого використання програм надає адміністраторові механізм ідентифікації програм, що запускають у домені, і керування можливостями виконання цих програм. Ці політики дозволяють адміністраторові запобігти виконанню небажаних застосувань, у тому числі вірусів і «троянських коней», а також програм, про які відомо, що після їхньої установки виникають конфлікти. Інформація про ці застосування передається за допомогою зазначення шляху до файлу, хешу файлу, підписаного сертифіката Microsoft Authenticode або зони безпеки в Інтернеті.

Використання інструментів в процесі керування безпекою ОС Microsoft Windows XP Professional наведено в табл. 1.

Таблиця 1 – Матриця вибору інструментів групової політики, secedit і засобів аналізу й налаштування безпеки

№ з/п	Процес	Active Directory використовується	Active Directory не використовується
1	Налаштування	Group Policy (Групова політика) secedit.exe Консоль Security Configuration and Analysis (Аналіз і налаштовування безпеки)	Консоль Security Configuration and Analysis (Аналіз і налаштовування безпеки) secedit.exe
2	Аналіз	Консоль Security Configuration and Analysis (Аналіз і налаштовування безпеки) secedit.exe	Консоль Security Configuration and Analysis (Аналіз і налаштовування безпеки) secedit.exe
3	Аудит	Консоль Security Configuration and Analysis (Аналіз і налаштовування безпеки) secedit.exe	Консоль Security Configuration and Analysis (Аналіз і налаштовування безпеки) secedit.exe
4	Обслуговування	Group Policy (Групова політика)	Консоль Security Configuration and Analysis (Аналіз і налаштовування безпеки) secedit.exe Консоль Local Security Policy (Локальна політика безпеки)
5	Редагування шаблонів безпеки	Оснащення Security Templates (Шаблони безпеки)	

При настроюванні параметрів безпеки за розділами, які наведено в [3], необхідним є застосування всіх зазначених вище інструментів і значний обсяг часу. Кількість параметрів, які необхідно перевірити та встановити потрібні значення, більш ніж 400. Природнім представляється необхідність створення адміністративної утиліти, яка б забезпечила автоматизацію конфігурування параметрів безпеки ОС.

III Опис адміністративної утиліти із конфігурації параметрів безпеки ОС Microsoft Windows XP Professional SP2

При розробці адміністративної утиліти із конфігурації параметрів безпеки ОС ставились наступні умови. Утиліті залежно від режиму роботи необхідно реалізовувати:

- конфігурування системи безпеки ОС Microsoft Windows XP Professional SP2 відповідно до вимог документа "Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2. Інсталяція об'єкта експертизи та конфігурування параметрів безпеки" [3];
- аналіз системи безпеки ОС Windows XP Professional SP2 на відповідність вимогам [3].

Утиліта повинна:

- одержувати на вхід дані про режим роботи й додаткові параметри;
- здійснювати перевірку коректності вхідних даних і при наявності помилки виводити довідку про параметри входу;
- перевіряти змінні середовища для визначення версії поточної операційної системи (робота тільки для Microsoft Windows XP Professional з Service Pack 2);
- містити довідку про застосування;
- зберігати та виводити результати аналізу на друк;
- мати можливість розширення й зміни вбудованих функцій.

Вхідні дані утиліти наступні:

- режим роботи – конфігурування або аналіз;
- клас АС – 1, 2, 3;
- ім'я файлу звіту – будь-яке ім'я файлу, що задовольняє вимогам іменування в ОС Microsoft Windows XP Professional.

За результатами роботи утиліти повинен створюватися файл звіту із заданим ім'ям, де буде зазначено: відомості про процес конфігурування або про відповідність аналізованої системи вимогам документа [3].

Дослідження щодо способу реалізації поставленої задачі показали наступне.

Перша спроба звести всі настроювання до змін у реєстрі виявилася невдалою, оскільки декілька розділів параметрів безпеки [3] (наприклад параметри локальної політики й політика обмеженого використання програм) не відображаються в документованих параметрах реєстру. Після детального дослідження було встановлено, що параметри розділів 1 - 6 можуть бути визначені централізовано – через відповідний шаблон безпеки. У той же час, адміністративні шаблони ОС Microsoft Windows XP Professional фактично містять настроювання реєстру, доступ до яких може бути отриманий лише через редактор «Локальна політика безпеки» – для редагування локального об'єкта групової політики Microsoft Windows XP Professional або через редактор групової політики – для редагування групових політик у централізованій базі даних Active Directory домену Microsoft Windows Server 2003.

Файли адміністративних шаблонів (*.adm) використовуються для налаштування параметрів реєстру ОС Microsoft Windows XP Professional SP2, що впливають на поведінку багатьох служб, застосувань і компонентів операційної системи.

Для налаштування параметрів використовуються наступні файли адміністративних шаблонів:

а) System.adm - містить параметри для налаштування середовища користувача;
б) Inetres.adm - містить параметри для Internet Explorer;
в) Conf.adm - містить параметри для NetMeeting;
г) Wmplayer.adm - містить параметри для Windows Media Player;
д) Wuau.adm - містить параметри для Windows Update.

Параметри налаштування адміністративних шаблонів діляться на дві групи:

- параметри налаштування комп'ютера, для збереження яких використовується кущ реєстру HKEY_LOCAL_MACHINE;
- параметри налаштування користувача, для збереження яких використовується кущ реєстру HKEY_CURRENT_USER.

Параметри налаштування комп'ютера мають перевагу перед аналогічним параметром користувача. Параметри користувача застосовуються до організаційного підрозділу, до якого входять користувачі, за допомогою зв'язаного об'єкта групової політики.

З метою створення єдиного інструмента конфігурування всі настроювання, зафіксовані в адміністративних шаблонах, були представлені у вигляді відповідних ключів реєстру.

В результаті всі зазначені настроювання безпеки, за винятком параметрів обмеженого використання програм, були представлені у вигляді двох конфігураційних файлів для кожного класу автоматизованої

системи:

- шаблону безпеки;
- шаблону настроювань реєстру, що відповідають параметрам адміністративних шаблонів.

Слід зазначити, що в ОС Microsoft Windows XP Professional настроювання, пов'язані з адміністративними шаблонами зберігаються у файлах політик безпеки %system root%\system32\GroupPolicy\ User\Registry.pol і %system root%\system32\GroupPolicy\Machine\Registry.pol, які по-перше, заборонено змінювати, а, по-друге, при копіюванні на інший комп'ютер функціонують некоректно.

При аналізі наведених в [3] параметрів настроювання були виявлені недоліки й неточності. Наприклад, не зазначені параметри, які використовуються при налаштуванні звітів про помилки, про збір додаткових файлів і інформації про комп'ютер. При виникненні подібних невідповідностей значення вибиралися за принципом максимального посилення безпеки.

При здійсненні вибору середовища і мови програмування було враховано наступне.

З урахуванням специфіки задачі – інструмент повинен застосовуватися тільки адміністратором системи, бути максимально простим, функціональним і легко розширюваним – утиліту доцільно реалізувати у вигляді консольного застосування.

Для створення програми спочатку планувалося використати інструментальне середовище Borland Delphi, в якому існує можливість створення консольних прикладних програм і є вбудовані засоби роботи з реєстром. Однак, компіляція в машинний код для поставленої задачі є скоріше недоліком, оскільки можливість розширення функціональності може бути досягнута тільки при постійній наявності вихідного коду й компілятора, також слід враховувати необхідність розбору текстових виразів при роботі утиліти. Приймаючи до уваги вищенаведене, було обрано середовище та мова програмування - Microsoft Visual Basic Scripting Edition. Додатковим аргументом на користь такого вибору стала наявність включеного в дистрибутив ОС Microsoft Windows XP сервера макросів Windows Script Host, здатного, зокрема, виконувати код Visual Basic Script.

Visual Basic Scripting Edition – це мова програмування, призначена для створення скриптів. Вона широко використовується при створенні скриптів в операційних системах сімейства Windows. Синтаксис Visual Basic Script є трохи спрощеною версією звичайного синтаксису Visual Basic. Зокрема, в Visual Basic Script не підтримується типізація: всі змінні мають тип Variant. Скрипт, написаний на Visual Basic Script, являє собою файл із розширенням .vbs, який ОС Windows сприймає як набір інструкцій і виконується сервером сценаріїв ОС Windows, що ставиться або оновлюється разом з Windows або з Internet Explorer.

Ідея скриптингу проста – складна система «збирається» з «елементарних», ефективно реалізованих, бінарних «об'єктів-цеглинок», які «з'єднуються» між собою за допомогою мови програмування високого рівня з інтерпретацією, добре пристосованою для рішення завдань «цементування програмної конструкції». Природно, що такий підхід пред'являє й підвищені вимоги до операційної системи, а саме – до механізмів взаємодії, до їхньої надійності, продуктивності й стандартизації.

У такого підходу існують як позитивні (не потрібно додаткових інструментів для інтерпретації й виконання, скрипти не компілюються під час написання), так і негативні моменти (відсутність візуального інтерфейсу, незручність налагодження).

Крім того, застосування Visual Basic Script для створення адміністративних скриптів обґрунтовано реалізацією в мові взаємодії із засобами Windows Management Instrumentation (WMI), можливості яких використані при створенні програмного забезпечення.

Інструментарій керування WMI є реалізацією корпорації Microsoft протоколу WBEM (Web-Based Enterprise Management – керування підприємством на основі веб-технологій), що регламентує стандарти загального доступу до даних керування через мережу підприємства. WMI забезпечує вбудовану підтримку моделі CIM (Common Information Model – загальна модель даних), якій мають відповідати об'єкти середовища керування.

WMI включає CIM-сумісну базу даних, у якій зберігаються визначення об'єктів і диспетчер об'єктів CIM, в задачі якого входить занесення об'єктів у сховище і керування ними, а також збір даних від постачальників WMI. Постачальники WMI відіграють роль посередників між WMI і компонентами операційної системи, застосуваннями та іншими системами. Постачальники надають не тільки дані, але і методи, за допомогою яких можливо керувати компонентами, властивості, що можуть бути змінені, і події, що інформують про зміни, які відбуваються в компонентах.

WMI може використовуватися засобами керування комп'ютерами, такими як Microsoft Systems Management Server. Крім того, WMI застосовується в інших технологіях, таких як Microsoft Health Monitor і Microsoft Operations Manager, а також сторонніми виробниками комп'ютерних систем керування. Можливо також використовувати WMI разом із системами програмування (такими як Windows Script Host)

як для одержання відомостей про конфігурацію комп'ютерних систем, у тому числі про серверні застосування, так і для зміни конфігурації.

Спираючись на результати попередніх досліджень було розроблено адміністративну утиліту, загальний алгоритм роботи якої зображено на рис. 1.

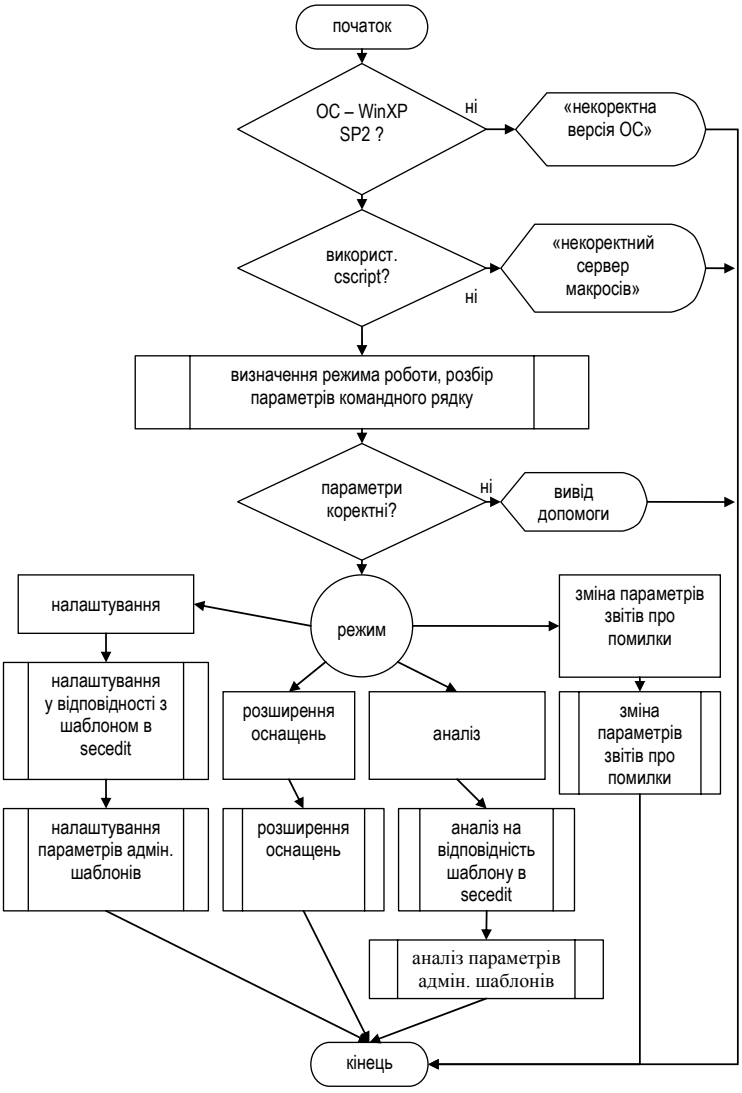

Рисунок 1 – Загальний алгоритм роботи утиліти

Далі наведемо опис розробленої утиліти.

Утиліта розроблена з використанням мови програмування Microsoft Visual Basic Script, засобів WMI і можливостей вбудованої утиліти secedit у вигляді скрипта.

Функції скрипта:

- налаштування параметрів безпеки ОС Microsoft Windows XP Professional SP2;
- аналіз параметрів безпеки ОС Microsoft Windows XP Professional SP2;
- розширення функціональності оснащень «Аналіз і налаштування безпеки» і «Локальні параметри безпеки»;
- збереження результатів роботи у файлі звіту;
- можливість розширення функціональності й доповнення вихідного коду програми без необхідності використання сторонніх трансляторів.

Реалізація утиліти у вигляді скрипта дозволяє забезпечити довільний вибір каталогу інсталяції. Для установки програми досить скопіювати всі файли дистрибутива в довільний каталог. Дистрибутив

програми містить наступні файли:

а) expsec.vbs – основний файл-скрипт;
б) expsec1.inf, expsec2.inf, expsec3.inf – шаблони безпеки, які використовуються при виклику команди secedit для відповідного класу АС;
в) usersec1.inf, usersec2.inf, usersec3.inf – параметри настроювання реєстру, які взяті з адміністративних шаблонів;
г) snapin.inf – файл для розширення оснащень «Аналіз і налаштування безпеки» і «Локальні параметри безпеки» шляхом забезпечення доступу з них до додаткових настроювань системи безпеки;
д) expsecparam.ini – параметри безпеки, які індивідуальні для кожної системи й не зазначені в рекомендаціях [3].

Запуск програми здійснюється з командного інтерпретатора ОС (cmd.exe) з наступним синтаксисом.

```
cscript expsec.vbs {/c|/a|/p|/e} /s:клас АС [/l:ім'я_файлу] [/d:ім'я_файлу]
```

Команда cscript вказує на необхідність застосування консольного варіанта сервера макросів (до складу Windows Script Host входить також варіант, що працює у віконному режимі – wscript). Призначення параметрів зазначено в табл. 2.

Таблиця 2 – Параметри скрипта expsec.vbs

Параметр	**Опис**
	РЕЖИМ РОБОТИ
/c	конфігурування політики безпеки комп'ютера
/a	аналіз політики безпеки комп'ютера
/p	перечитати файл змінюваних параметрів
/e	розширити перелік параметрів оснащень
	ПАРАМЕТРИ
/s: клас	клас АС, для якого проводиться конфігурування або аналіз
/d: ім'я_файлу	файл бази параметрів безпеки secedit (значення за замовчуванням – expsecdb)
/l: ім'я_файлу	файл звіту (значення за замовчуванням – expseclog [час_дата] .log)

У випадку, якщо при зазначенні параметрів допущена помилка, а також, якщо як ключ зазначений /? або скрипт викликаний без параметрів, виводиться довідкове повідомлення.

Якщо параметри зазначені правильно, у вікні командного інтерпретатора відображається режим роботи, а також, залежно від режиму використання, – клас АС, для якого проводиться аналіз або налаштування, ім'я файлу бази параметрів безпеки, ім'я файлу звіту.

Режим /p використовується, якщо змінилися параметри звітів про помилки й внесені відповідні зміни у файл expsecparam.ini:

- шлях до каталогу зберігання звітів;
- адреса служби оновлень в локальній мережі для пошуку оновлень;
- сервер статистики в локальній мережі.

Режим /e застосовується для внесення додаткових параметрів (містяться у файлі snapin.inf) в оточення оснастки «Аналіз і налаштування безпеки» і «Локальні параметри безпеки», а саме в підрозділ «Параметри безпеки». Всі внесені доповнення специфіковані в [3]. Таким чином, досягається можливість візуального внесення змін у параметри без використання додаткового інструментарію й адміністративних шаблонів.

Параметр /d вказує на ім'я створюваного або використовуваного файлу бази параметрів безпеки команди secedit, що викликається зі скрипта для застосування шаблона безпеки до відповідного класу АС (expsec1.inf, expsec2.inf, expsec3.inf) при конфігуруванні на підставі такого шаблона.

Параметр /l вказує на ім'я створюваного файлу звіту. При застосуванні шаблона безпеки команда secedit фіксує в цьому файлі хід своєї роботи, після чого продовжує роботу скрипт, який застосовує до системи параметри налаштування реєстру, які взяті з адміністративних шаблонів (usersec1.inf, usersec2.inf, usersec3.inf), і фіксує цей процес у тому ж файлі звіту. Наприкінці звіту вноситься підсумкова інформація з обох етапів конфігурування.

У зв'язку з використанням різноманітного програмного забезпечення в конкретних організаціях в утиліту не включена можливість настроювання політики обмеженого використання програм, доступ до якої здійснюється через оснастку «Локальні параметри безпеки». Загальні рекомендації з обмеженого використання програм відповідно до [3] полягають у наступному.

Адміністратор спочатку визначає набір програм, які дозволяється запускати на клієнтських

комп'ютерах, а потім встановлює обмеження, які будуть застосовуватися до клієнтських комп'ютерів.

Політика обмеженого використання програм в початковому вигляді складається із заданого за умовчанням рівня безпеки для необмежених або заборонених параметрів і правил, визначених для об'єкта групової політики. Політика може застосовуватися в домені для локальних комп'ютерів або користувачів.

Політики обмеженого використання програм застосовуються для виконання наступних дій:

- визначення програм, дозволених для запуску на клієнтських комп'ютерах;
- обмеження доступу користувачів до конкретних файлів на комп'ютерах, які мають декілька користувачів;
- визначення кола користувачів, які мають дозвіл додавати до клієнтських комп'ютерів довірених видавців;
- визначення впливу політики на всіх користувачів або тільки користувачів на клієнтських комп'ютерах;
- заборона запуску виконавчих файлів на локальному комп'ютері, в підрозділі, вузлі або домені.

Політика обмеженого використання програм містить дві компоненти:

- задані за умовчанням правила;
- список виключень з цих правил.

Для правил за умовчанням можна встановити значення «Необмежений» або «Заборонений». Установка для правила значення «Необмежений» дозволяє адміністратору визначити виключення або набір програм, які заборонено запускати. Більш безпечний підхід – встановити значення «Заборонений», а потім визначити набір програм, які дозволяється запускати.

Більш детально рекомендовані правила зазначені в [3].

IV Методика застосування адміністративної утиліти із конфігурації параметрів безпеки ОС Microsoft Windows XP Professional SP2

Для використання утиліти необхідно дотримуватися наступних рекомендацій. Перш за все треба врахувати, що скрипт призначено для роботи в середовищі Microsoft Windows XP Professional SP2 і для його коректного використання необхідні права адміністратора.

1. ***Установка.***
   1.1. Створити новий каталог на жорсткому диску.
   1.2. Скопіювати всі файли у створений каталог.
2. ***Визначення параметрів звітів про помилки.***
   2.1. Встановити необхідні значення наступних параметрів: шлях до каталогу зберігання звітів; адреса служби оновлень в локальній мережі для пошуку оновлень; сервер статистики в локальній мережі.
   2.2. Внести відповідні значення у файл expsecparam.ini.
3. ***Аналіз.***
   3.1. Визначити клас АС для поточної системи.
   3.2. Визначити ім'я бази параметрів безпеки secedit.
   3.3. Визначити ім'я файлу звіту.
   3.4. Запустити скрипт у режимі /a з визначеними раніше параметрами.
4. ***Конфігурування.***
   4.1. Визначити клас АС для поточної системи.
   4.2. Визначити ім'я бази параметрів безпеки secedit.
   4.3. Визначити ім'я файлу звіту.
   4.4. Запустити скрипт у режимі /c з визначеними раніше параметрами.
5. ***Розширення оснащень і їхнє використання.***
   5.1. Запустити скрипт у режимі /e.
   5.2. У підрозділі «Параметри безпеки» оснащень «Аналіз і налаштування безпеки» і «Локальні параметри безпеки» налаштувати або проаналізувати параметри системи.
6. ***Зміна параметрів звітів про помилки.***
   6.1. Внести зміни у файл expsecparam.ini.
   6.2. Запустити скрипт у режимі /p.
7. ***Налаштування політики обмеженого використання програм.***
   7.1. Налаштувати загальні параметри за допомогою розділу «Політики обмеженого використання програм» оснащення «Локальні параметри безпеки».
   7.2. Визначити програми, доступ до яких має бути обмеженим на підставі політики безпеки.

7.3. Налаштувати ці обмеження.

V Висновки

Результати виконаних досліджень і розроблена утиліта після можливої сертифікації (або отримання позитивного експертного висновку) дозволять, по-перше, в процесі створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах державних організацій застосувати на практиці рекомендації з конфігурування параметрів безпеки ОС Microsoft Windows XP Professional SP2, і по-друге, в процесі контрольно–інспекційної роботи здійснювати перевірку параметрів безпеки ОС Microsoft Windows XP Professional SP2.

*Література: **1**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Експертний висновок. **2**. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. **3**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Інсталяція об'єкта експертизи та конфігурування параметрів безпеки. **4**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Технічні вимоги. **5**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Ідентифікація об'єкта експертизи під час проведення періодичних перевірок стану захищеності. Рекомендації. **6**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Оновлення інстальованого програмного забезпечення об'єкта експертизи. Рекомендації.*

УДК 681.5:621.391

ОСНОВНІ ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДКРИТИХ СИСТЕМ. Частина 2. ВЛАСТИВОСТІ ВІДКРИТИХ СИСТЕМ ТА ВИМОГИ ДО ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ

Володимир Кононович, Ірина Кононович*, Тетяна Тардаскіна**

*Одеський регіональний центр технічного захисту інформації ВАТ "Укртелеком", *Інститут комп'ютерних технологій ОДАХ, **Одеська національна академія зв'язку*

Анотація: **Аналізуються новітні науково-технічні досягнення у області інформатики, інформаційних технологій та виводяться основні принципи інформаційної безпеки відкритих систем, що характеризуються інтелектульним управлінням й активною взаємодією з іншими системами. Виявляються властивості відкритих систем та формульються вимоги до інтелектуального управління з точки зору їх інформаційної безпеки.**

Summary: **The newest scientific-technical achievements in informatics, information technologies and main principles of information security open systems, which characterized intellectual control and active interaction with other systems, are analyzed. Properties of open system are defined are formulated for intellectual control of them from the point of view of their information security.**

Ключові слова: **Інформаційна безпека, відкриті системи, інформодинаміка, інформатика, система управління, інтелектуальне управління, числення предикатів.**

I Вступ

Дане дослідження стосується сфери технічного захисту інформації та інформаційної безпеки систем, які об'єднуються під загальною назвою – інформаційні технології. Проблематика дослідження, аналіз досягнень та публікацій наведені в частині 1 цієї роботи [1]. *Аналіз останніх досягнень і публікацій* показує, що моделі системи процесів захисту інформації [2], інформації, як управління процесами відкритих систем, теорії інформодинаміки [3], та керованості й спостережності систем у сучасній теорії управління [4] мають дещо суттєве-спільне, що вимагає уважного дослідження. Відкриті системи існують лише як процес. Ізоляція відкритої системи від зовнішніх взаємодій приводить до її деградації. Нова парадигма інформаційної безпеки, що розвивається в США, розглядає інформаційні системи як принципово відкриті, де синергетика гомеостазу (стану усталеної рівноваги) визначається балансом