Додаток №4
до Договору про надання доступу
до Інформаційної
системи портового співтовариства
від «___» _____ 2014 року

І Н С Т Р У К Ц І Я

з інсталяції та конфігурування параметрів безпеки ОС
Windows XP Professional SP2

Вступ

Корпорація Microsoft разом з носієм ОС Windows XP Professional SP2 постачає документацію, яка містить детальні інструкції щодо установки ОС та додаткові відомості.

Інструкції щодо установки та інші відомості, які наведені в цих документах рекомендується використовувати під час установки ОС Windows XP Professional SP2 на АРМ користувачів.

В документі розглядається конфігурування параметрів безпеки операційної системи Windows XP Professional SP2.

Значення параметрів безпеки наведені в табл. 1-20. Для параметрів, які несуттєві для безпеки, значення не вказані.

1 Засоби, які використовуються для конфігурування параметрів безпеки

Для конфігурування параметрів безпеки застосовуються вбудовані системні компоненти ОС Windows XP Professional SP2 такі як:

- Редактор групових політик (далі редактор політики);
- Редактор реєстру.

1.1 Запуск редактора політик

Запуск редактора політики здійснюється шляхом виконання в командному рядку команди «gpedit.msc».

1.2 Запуск редактора реєстру

Запуск редактора реєстру здійснюється шляхом виконання в командному рядку команди «regedit.exe».

2 Політика облікових записів

Політика облікових записів містить параметри безпеки для паролів і блокування облікових записів.

2.1 Політика паролів

Параметри налаштовуються за допомогою редактора політики за адресою:
Конфігурація комп'ютера\ Конфігурація Windows\ Параметри безпеки\ Політика облікових записів\ Політика паролів

Параметри наведені в табл. 1.

Таблиця 1

№ п/п	Назва параметра	Параметр (Установка)
1	Вимагати неповторюваність паролів (Enforce password history)	24 збережених паролів (24 passwords remembered)
2	Максимальний термін дії пароля (Maximum password age)	42 дні (42 days)
3	Мінімальний термін дії пароля (Minimum password age)	30 днів (30 days)
4	Мінімальна довжина пароля (Minimum password lengths)	8

№ п/п	Назва параметра	Параметр (Установка)
5	Пароль повинен відповідати вимогам складності (Password must meet complexity requirements)	Включений (Enabled)
6	Зберігати паролі всіх користувачів у домені, використовуючи зворотне шифрування (Store password using reversible encryption for all users in the domain)	Відключений (Disabled)

2.2 Політика блокування облікового запису

Параметри налаштовуються за допомогою редактора політики за адресою:

Конфігурація комп'ютера\ Конфігурація Windows\ Параметри безпеки\ Політики облікових записів\ Політика блокування облікового запису

Параметри наведені в табл. 2.

Таблиця 2

№ п/п	Назва параметра	Параметр (Установка)
1	Блокування облікового запису на (Account lockout duration)	30 хвилин (30 minutes)
2	Граничне значення блокування (Account lockout duration)	10 помилок входу до системи (10 invalid logon attempts)
3	Скидання лічильника блокування через (Reset account lockout counter after)	30 хвилин (30 minutes)

3 Параметри локальної політики

3.1 Політика аудиту

Параметри налаштовуються за допомогою редактора політики за адресою:

Конфігурація комп'ютера\ Конфігурація Windows\ Параметри безпеки\ Локальні політики\ Політика аудиту

Параметри наведені в табл. 3.

Таблиця 3

№ п/п	Назва параметра	Параметр (Установка)
1	Аудит входу до системи (Audit account logon events)	Успіх, Відмова (Success, Failure)
2	Аудит керування обліковими записами (Audit account management)	Успіх, Відмова (Success, Failure)
3	Аудит доступу до служби каталогів (Audit directory service access)	Немає аудита (No auditing)
4	Аудит подій входу в систему (Audit logon events)	Успіх, Відмова (Success, Failure)
5	Аудит доступу до об'єктів (Audit object access)	Успіх, Відмова (Success, Failure)
6	Аудит зміни політики (Audit policy change)	Успіх (Success)
7	Аудит використання привілеїв (Audit privilege use)	Відмова (Failure)
8	Аудит відстеження процесів (Audit process traking)	Немає аудиту (No auditing)
9	Аудит системних подій (Audit system events)	Успіх, Відмова (Success, Failure)

3.2 Параметри призначення прав користувачів

Параметри налаштовуються за допомогою редактора політики за зазначеною адресою:

Конфігурація комп'ютера\ Конфігурація Windows\ Параметри безпеки\ Локальні політики\ Призначення прав користувачів

Параметри наведені в табл. 4.

Таблиця 4

№ п/п	Назва параметра	Параметр (Установка)
1	Доступ до комп'ютера з мережі (Access this computer from the network)	Не визначено (Not defined) /Ніхто (No One)
2	Робота в режимі операційної системи (Act as part of the operating system)	Ніхто (No One)
3	Додавання робочих станцій до домену (Add workstations to domain)	Не визначено (Not defined) / Ніхто (No One)
4	Настроювання квот пам'яті для процесу (Adjust memory quotas to a process)	Адміністратори (Administrators), LOCAL SERVICE
5	Дозволяти вхід у систему через службу терміналів (Allow logon through Terminal Service)	Не визначено (Not defined) / Ніхто (No One)
6	Архівування файлів і каталогів (Back up files and directories)	Адміністратори (Administrators)
7	Обхід перехресної перевірки (Bypass traverse checking)	Користувачі Адміністратори (Users, Administrators)
8	Зміна системного часу (Change the system time)	Адміністратори (Administrators)
9	Створення сторінкового файлу (Create a pagefile)	Адміністратори (Administrators)
10	Створення маркерного об'єкта (Create a token object)	Ніхто (No one)
11	Створення постійних об'єктів спільного використання (Create permanent shared objects)	Ніхто (No one)
12	Налагодження програм (Debug programs)	Ніхто (No one)
13	Відмова в доступі до комп'ютера з мережі (Deny access to this computer from the network)	Не визначено (Not defined) / Всі, АНОНІМНИЙ ВХІД (Everyone, ANONYOMUS LOGON)
14	Відмова у вході як пакетне завдання (Deny logon as a batch job)	Не визначено (Not defined)
15	Відмова у вході як служба (Deny logon as a service)	Не визначено (Not defined)
16	Відхилити локальний вхід (Deny logon locally)	Support_388945a, Guest, Any service accounts
17	Заборонити вхід у систему через службу терміналів (Deny logon through Terminal Services)	Не визначено (Not defined) Всі, АНОНІМНИЙ ВХІД (Everyone, ANONYOMUS LOGON)
18	Дозвіл довіри до облікових записів при делегуванні (Eanble computer and user accounts to be trusted for delegation)	Ніхто (No one)
19	Примусове вилучення завершення (Force shutdown from a remote system)	Не визначено (Not defined) / Ніхто (No one)
20	Створення журналів безпеки (Generate security audits)	LOCAL SERVICE

№ п/п	Назва параметра	Параметр (Установка)
21	Збільшення пріоритету диспетчерування (Increase scheduling priority)	Адміністратори (Administrators)
22	Завантаження й вивантаження драйверів пристроїв (Load and unload device drivers)	Адміністратори (Administrators)
23	Закріплення сторінок у пам'яті (Lock pages in memory)	Не визначено (Not defined)
24	Вхід як пакетне завдання (Log on as a batch job)	Ніхто (No one)
25	Вхід як служба (Log on as a service)	Ніхто (No one)
26	Локальний вхід у систему (Log on locally)	Адміністратори Користувачі, (Administrators, Users)
27	Керування аудитом і журналом безпеки (Manage auditing and security log)	Адміністратори (Administrators)
28	Зміна параметрів середовища устаткування (Modify firmware environment values)	Адміністратори (Administrators)
29	Запуск операцій по обслуговуванню тому (Perform volume main tence tasks)	Адміністратори (Administrators)
30	Профілювання одного процесу (Profile single process)	Адміністратори (Administrators)
31	Профілювання завантаженості системи (Profile system performance)	Адміністратори (Administrators)
32	Витягання комп'ютера зі стикувального вузла (Remove computer from docking station)	Не визначено (Not defined) Адміністратори Користувачі (Administrators, Users)
33	Заміна маркера рівня процесу (Replace a process level token)	LOCAL SERVICE
34	Відновлення файлів і каталогів (Restore files and directories)	Адміністратори (Administrators)
35	Завершення роботи системи (Shut down the system)	Адміністратори, Користувачі (Administrators, Users)
36	Синхронізація даних служби каталогів (Synchronize directory service data)	Не визначено (Not defined)
37	Оволодіння файлами або іншими об’єктами (Take ownership of files or other objects)	Адміністратори (Administrators)

3.3 Параметри безпеки

Параметри налаштовуються за допомогою редактора політики за адресою:
Конфігурація комп'ютера\ Конфігурація Windows\ Параметри безпеки\ Локальні політики\ Параметри безпеки

Параметри наведені в табл. 5.

Таблиця 5

№ п/п	Назва параметра	Параметр (Установка)
1	Облікові записи: стан облікового запису Адміністратор (Accounts: Administrator account status)	Відключений (Disabled)
2	Облікові записи: стан облікового запису Гість	Відключений

№ п/п	Назва параметра	Параметр (Установка)
	(Accounts: Guest account status)	(Disabled)
3	Облікові записи: обмежити використання порожніх паролів тільки для консольного входу (Accounts: Limit local account use of blank passwords to console logon only)	Включений (Enabled)
4	Облікові записи: Перейменування облікового запису адміністратора (Accounts: Rename administrator account)	Рекомендується перейменування облікового запису
5	Облікові записи: Перейменування облікового запису гостя (Accounts: Rename guest account)	Рекомендується перейменування облікового запису
6	Аудит: Аудит доступу глобальних системних об'єктів (Audit: Audit the access of global system objects)	Включений (Enabled)
7	Аудит: Аудит прав на архівацію й відновлення (Audit: Audit the use of Backup and Restore privilege)	Включений (Enabled)
8	Аудит: Негайне відключення системи, якщо неможливо внести в журнал запису про аудит безпеки (Audit: Shut down system immediately if unable to log security audits	Відключений (Disabled)
9	Пристрої: Дозволяти відстиковку без входу до системи (Devices: Allow undock without having to log on)	Відключений (Disabled)
10	Пристрої: Дозволено форматувати й витягати знімні носії (Devices: Allowed format and eject removable media)	Адміністратор (Administrators)
12	Пристрої: дозволити доступ до дисководів компакт-дисків тільки локальним користувачам (Devices: Restrict CD-ROM access to locally logged-on user only)	Відключений (Disabled)
13	Пристрої: дозволити доступ до дисководів гнучких дисків тільки локальним користувачам (Devices: Restrict floppy access to lcocally logged-on user only)	Відключений (Disabled)
14	Пристрої: поводження при установці непідписного драйвера (Devices: Unsigned driver installation behavior)	Не дозволяти установку (Do not allow installation)
15	Контролер домену: дозволити операторам сервера задавати виконання завдань за розкладом (Domain controller: Allow server operators to schedule tasks)	Не визначено (Not defined)
16	Контролер домену: Вимоги підписування для LDAP сервера (Domain controller: LDAP server signing requirements)	Не визначено (Not defined)
17	Контролер домену: Заборонити зміну пароля облікових записів комп'ютера (Domain controller: Refuse machine account password changes)	Не визначено (Not defined)
18	Член домену: Завжди потрібний цифровий підпис або шифрування потоку даних безпечного каналу (Domain member: Digitaly encrypt or sign secure channel data (always))	Не визначено (Not defined)
19	Член домену: Шифрування даних безпечного каналу, коли це можливо (Domain member: Digitally encrypt secure channel data	Не визначено (Not defined)

№ п/п	Назва параметра	Параметр (Установка)
	(when possible))	
20	Член домену: Максимальний термін дії пароля облікових записів комп'ютера (Domain member: Maximum machine account password age)	Не визначено (Not defined)
21	Член домену: Цифровий підпис даних безпечного каналу, коли це можливо (Domain member: Digitally sign secure channel data (when possible))	Не визначено (Not defined)
22	Член домену: Відключити заміну пароля облікових записів комп'ютера (Domain member: Disable machine account password changes)	Не визначено (Not defined)
23	Член домену: вимагає стійкого ключа сеансу (Domain member: Require strong (Windows 2000 or later) session key)	Не визначено (Not defined)
24	Інтерактивний вхід у систему: Не відображати останнього імені користувача (Interactive logon: Do not display last user name)	Включений (Enabled)
25	Інтерактивний вхід у систему: Не вимагати натискання CTRL+ALT+DEL (Interactive logon: Do not require CTRL+ALT+DEL)	Відключений (Disabled)
26	Інтерактивний вхід у систему: Текст повідомлення для користувачів при вході в систему (Interactive logon: Message text for users attempting to logon)	Вхід тільки для авторизованих користувачів.
27	Інтерактивний вхід у систему: Заголовок повідомлення для користувачів при вході в систему (Interactive logon: Message title for users attempting to logon)	ПРОДОВЖЕННЯ СПРОБ БЕЗ НАЛЕЖНОЇ АВТОРИЗАЦІЇ Є ЗЛОЧИНОМ
28	Інтерактивний вхід у систему: кількість попередніх підключень до кешу (у випадку відсутності доступу до контролера домену) (Interactive logon: Number of previous logons to cache (in case domain controller is not available))	Не визначено (Not defined)
29	Інтерактивний вхід у систему: нагадувати користувачам про витікання терміну дії пароля заздалегідь (Interactive logon: Prompt user to change password before expiration)	7 днів (7 days)
30	Інтерактивний вхід у систему: вимагати перевірки на контролері домену для скасування блокування робочої станції (Interactive logon: Require Domain controller authentication to unlock workstation)	Відключений (Disabled)
31	Інтерактивний вхід у систему: поводження при добуванні смарт-карти (Interactive logon: Smart card removal behavior	Блокування робочої станції (Lock Workstation)
32	Клієнт мережі Microsoft: використати цифровий підпис (завжди) (Microsoft network client: Digitally sign communications (always))	Не визначено (Not defined)
33	Клієнт мережі Microsoft: використати цифровий підпис (за згодою сервера) (Microsoft network client: Digitally sign communications (if server agrees))	Не визначено (Not defined)

№ п/п	Назва параметра	Параметр (Установка)
34	Клієнт мережі Microsoft: посилати незашифрований пароль стороннім SMB-серверам (Microsoft network client: Send unencrypted password to third-party SMB servers)	Не визначено (Not defined)
35	Сервер мережі Microsoft: тривалість простою перед відключенням сеансу (Microsoft network server: Amount of idle time required before suspending session)	Не визначено (Not defined)
36	Сервер мережі Microsoft: Використати цифровий підпис (завжди) (Microsoft network server: Digitally sign communications (always))	Не визначено (Not defined)
37	Сервер мережі Microsoft: Використати цифровий підпис (за згодою клієнта) (Microsoft network server: Digitally sign communications (if client agrees))	Не визначено (Not defined)
38	Сервер мережі Microsoft: відключати клієнтів після закінчення дозволених годин входу (Microsoft network server: Disconnect clients when logon hours expire)	Не визначено (Not defined)
39	Доступ до мережі: Дозволити трансляцію анонімного SID в ім'я (Network access: Allow anonymous SID/Name translation)	Не визначено (Not defined)
40	Мережний доступ: Не дозволяти перерахування облікових записів SAM анонімним користувачам (Network access: Do not allow anonymous enumeration of SAM accounts)	Не визначено (Not defined) / Включений (Enabled)
41	Мережний доступ: не дозволяти перерахування облікових записів SAM і загальних ресурсів анонімним користувачам (Network access: Do not allow anonymous enumeration of SAM accounts and shares)	Не визначено (Not defined) / Включений (Enabled)
42	Мережний доступ: не дозволяти збереження облікових даних або цифрових паспортів .NET для мережної перевірки дійсності користувача (Network access: Do not allow storage of credentials or .NET Passports for network authentication)	Не визначено (Not defined) / Включений (Enabled)
43	Мережний доступ: Дозволяти застосування дозволів для всіх до анонімних користувачів (Network access: Let Everyone permissions apply to anonymous users)	Не визначено (Not defined) / Включений (Enabled)
44	Мережний доступ: Дозволяти анонімний доступ до іменованих каналів (Network access: Named Pipes that can be accessed anonymously)	Не визначено (Not defined)
45	Мережний доступ: Дозволяти анонімний доступ до загальних ресурсів (Network access: (Shares that can be accessed anonymously)	Відключений (Disabled)
46	Мережний доступ: Шляхи в реєстрі доступні через вилучене підключення (Network access: Remotely accessible registry paths)	Не визначено (Not defined)

№ п/п	Назва параметра	Параметр (Установка)
47	Мережний доступ: Модель спільного доступу й безпеки для локальних облікових записів (Network access: Sharing and security model for local accounts)	Не визначено (Not defined)
48	Мережна безпека: не зберігати хеш - значень LAN Manager при наступній зміні пароля (Network security: do not store LAN Manager hash value on next password change)	Не визначено (Not defined)
49	Мережна безпека: примусовий вивід із сеансу після закінчення припустимих годин роботи (Network security: Force logoff when logon hours expire)	Не визначено (Not defined)
50	Мережна безпека: рівень перевірки дійсності LAN Manager (Network security: LAN Manager authentication level)	Не визначено (Not defined)
51	Мережна безпека: Вимоги підписування для LDAP клієнта (Network security: LDAP client signing requirements)	Не визначено (Not defined)
52	Мережна безпека: Мінімальна сеансова безпека для клієнтів на базі NTLM SSP (включаючи безпеку RPC) (Network security: Minimum session security for NTLM SSP based (including secure RPC) clients)	Не визначено (Not defined)
53	Мережна безпека: Мінімальна сеансова безпека для серверів на базі NTLM SSP (включаючи безпеку RPC) (Network security: Minimum session security for NTLM SSP based (including secure RPC) servers)	Не визначено (Not defined)
54	Консоль відновлення: Дозволити автоматичний вхід адміністратора (Recovery console: Allow automatic administrative logon)	Відключений (Disabled)
55	Консоль відновлення: Дозволити копіювання дискет і доступ до всіх дисків та папок Адміністратора (Recovery console: Allow floppy copy and access to all drives and all folders)	Відключений (Disabled)
56	Завершення роботи: дозволити завершення роботи системи без виконання входу в систему (Shutdown: Allow system to be shutdown without having to log on)	Відключений (Disabled)
57	Завершення роботи: Очищення сторінкового файлу віртуальної пам'яті (Shutdown: Clear virtual memory pagefile)	Включений (Enabled)
58	Системна криптографія: Використати FIPS-сумісні алгоритми для шифрування, хешування й підписування (System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing)	Відключений (Disabled)
59	Системні об'єкти: Власник за замовчуванням для об'єктів, створених членами групи адміністраторів (System objects: Default owner for objects created by members of the Administrators group)	Творець об'єкта (Object creator)
60	Системні об'єкти: Ураховувати регістр для підсистем, відмінних від Windows (Require case insensitivity for non-Windows subsystems)	Включений (Enabled)
61	Системні об'єкти: Підсилити дозвіл за замовчуванням для внутрішніх системних об'єктів (наприклад, символічних посилань)	Включений (Enabled)

№ п/п	Назва параметра	Параметр (Установка)
	(System objects: Strengthen default permissions of internal system objects (e.g. Symbolic links))	

4 Журнал подій

4.1 Параметри безпеки журналу подій

Параметри налаштовуються за допомогою редактора політики за адресою:

Конфігурація комп'ютера\ Конфігурація Windows\ Параметри безпеки\ Журнал подій

Параметри наведені в табл. 6.

Таблиця 6

№ п/п	Назва параметра	Параметр (Установка)
1	Максимальний розмір журналу додатків (Maximum application log size)	100032 Кбайт 100032 KB
2	Максимальний розмір журналу безпеки (Maximum security log size)	100032 Кбайт 100032 KB
3	Максимальний розмір системного журналу (Maximum system log size)	100032 Кбайт 100032 KB
4	Заборонити доступ локальної групи гостей до журналу додатків (Prevent local guests group from accessing application log)	Включений (Enabled)
5	Заборонити доступ локальної групи гостей до журналу безпеки (Prevent local guests group from accessing security log)	Включений (Enabled)
6	Заборонити доступ локальної групи гостей до системного журналу (Prevent local guests group from accessing system log)	Включений (Enabled)
7	Збереження подій у журналі додатків (днів) (Retention method for application log)	Не визначено (Not defined)
8	Збереження подій у журналі безпеки (днів) (Retention method for security log)	Не визначено (Not defined)
9	Збереження подій у системному журналі (днів) (Retention method for system log)	Не визначено (Not defined)
10	Збереження подій у журналі додатків (Retention method for application log)	У міру потреби (As Needed)
11	Збереження подій у журналі безпеки (Retention method for security log)	У міру потреби (As Needed)
12	Збереження подій у системному журналі (Retention method for system log)	У міру потреби (As Needed)

5 Системні служби

5.1 Параметри налаштування системних служб для комп'ютерів

Параметри налаштовуються за допомогою редактора політики за адресою:

Конфігурація комп'ютера\ Конфігурація Windows\ Параметри безпеки\ Системні служби

Параметри наведені в табл. 7.

Таблиця 7

№ п/п	Назва параметра	Параметр (Установка)

№ п/п	Назва параметра	Параметр (Установка)
1	Оповіщувач (Alerter)	Відключено (Disabled)
2	Служба шлюзу рівня додатків (Application Layer Gateway Service)	Відключено (Disabled)
3	Керування додатками (Application Management)	Вручну (Manual)
4	Machine Debug Manager	Відключено (Disabled)
5	Автоматичне відновлення (Automatic Updates)	Відключено (Disabled)
6	Фонова інтелектуальна служба передачі (Background Intelligent Transfer Service)	Відключено (Disabled)
7	Сервер папки обміну (ClipBook)	Відключено (Disabled)
8	Система подій COM+ (COM+ Event System)	Вручну (Manual)
9	Системний додаток COM+ (COM+ System Application)	Вручну (Manual)
10	Оглядач комп'ютерів (Computer Browser)	Відключено (Disabled)
11	Служби криптографії (Crytpographic Services)	Авто (Auto)
12	DHCP-клієнт (DHCP-client)	Відключено/Авто (Disabled/Auto)
13	Клієнт відстеження зв'язків, що змінилися (Distributed Link Tracking Client)	Вручну (Manual)
14	Координатор розподілених транзакцій (Distributed Transaction Coordinator)	Вручну (Manual)
15	DNS – клієнт (DNS Client)	Відключено/Авто (Disabled/Auto)
16	Служба реєстрації помилок (Error Reporting Service)	Авто (Auto)
17	Журнал подій (Event Log)	Авто (Auto)
18	Сумісність швидкого перемикання користувачів (Fast User Switching Compatibility	Відключено (Disabled)
19	Служба факсів (Fax)	Відключено (Disabled)
20	Довідка й підтримка (Help and Support)	Авто (Auto)
21	Доступ до HID - пристроїв (Human Interface Device Access)	Відключено (Disabled)
22	Служба COM запису компакт –дисків IMAPI (IMAPI CD-Burning COM Service)	Відключено (Disabled)
23	Служба індексування (Indexing Service)	Відключено (Disabled)
24	Брандмауер Інтернету (ICF)/Загальний доступ до Інтернету (ICS) (Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS))	Відключено (Disabled)
25	Служба IPSec (IPSec Services)	Авто (Auto)
26	Диспетчер логічних дисків	Вручну

№ п/п	Назва параметра	Параметр (Установка)
	(Logical Disk Manager	(Manual)
27	Служба адміністрування диспетчера логічних дисків (Logical Disk Manager Administrative Service)	Вручну (Manual)
28	Служба повідомлень (Messenger)	Відключено (Disabled)
29	Microsoft Software Shadow Copy Provider	Вручну (Manual)
30	Мережний вхід у систему (Net logon)	Відключено (Disabled)
31	Вилучене керування робочим столом в NetMeeting (NetMeeting Remote Desktop Sharing)	Відключено (Disabled)
32	Мережні підключення (Network connections)	Вручну (Manual)
33	Служба мережного DDE (Network DDE)	Відключено (Disabled)
34	Диспетчер мережного DDE (Network DDE DSDM)	Відключено (Disabled)
35	Служба мережного розташування (NLA) (Network Location Awareness (NLA))	Вручну (Manual)
36	Постачальник підтримки безпеки NTLM (NTLM Security Support Provider)	Авто (Auto)
37	Журнали оповіщення продуктивності (Performance Logs and Alerts)	Вручну (Manual)
38	Plug and Play	Авто (Auto)
39	Серійний номер переносного медіа-пристрою (Portable Media Serial Number)	Відключено (Disabled)
40	Диспетчер черги печатки (Print Spooler)	Авто (Auto)
41	Захищене сховище (Protected Storage)	Авто (Auto)
42	Qo RSVP	Відключено (Disabled)
43	Диспетчер Авто (Auto)- підключень вилученого доступу (Remote Access Auto Connection Manager)	Відключено (Disabled)
44	Диспетчер підключень вилученого доступу (Remote Access Connection Manager)	Відключено (Disabled)
45	Диспетчер сеансу довідки для вилученого робочого стола (Remote Desktop Help Session Manager)	Відключено (Disabled)
46	Вилучений виклик процедур (RPC) (Remote Procedure Call(RPC))	Авто (Auto)
47	Локатор вилученого виклику процедур (RPC) (Remote Procedure Call (RPC) Locator)	Вручну (Manual)
48	Вилучений реєстр (Remote Registry)	Відключено (Disabled)
49	Знімні ЗП (Removable Storage)	Відключено (Disabled)
50	Маршрутизація й вилучений доступ (Routing and Remote Access)	Відключено (Disabled)
51	Вторинний вхід у систему (Secondary Logon)	Авто (Auto)
52	Диспетчер облікових записів безпеки (Security Accounts Manager)	Авто (Auto)

№ п/п	Назва параметра	Параметр (Установка)
53	Сервер (Server)	Авто (Auto)
54	Визначення встаткування оболонки (Shell Hardware Detection)	Авто (Auto)
55	Смарт-карти (Smart Card)	Вручну (Manual)
56	Модуль підтримки смарт-карт (Smart Card Helper)	Вручну (Manual)
57	Служба виявлення SSDP (SSDP Discovery Service)	Відключено (Disabled)
58	Повідомлення про системні події (System Event Notification)	Авто (Auto)
59	Служба відновлення системи (System Restore Service)	Вручну (Manual)
60	Планувальник завдань (Task Scheduler)	Відключено (Disabled)
62	Телефонія (Telephony)	Відключено (Disabled)
63	Telnet	Відключено (Disabled)
64	Служби терміналів (Terminal Service)	Відключено (Disabled)
65	Теми (Themes)	Авто (Auto)
66	Джерело безперебійного живлення (UPS)	Вручну (Manual)
67	Вузол універсальних PnP-пристроїв (Universal Plug and Play Device Host)	Відключено (Disabled)
68	Диспетчер відвантаження (Upload Manager)	Вручну (Manual)
69	Тіньове копіювання тому (Volume Shadow Copy)	Вручну (Manual)
70	Веб-клієнт (WebClient)	Авто (Auto)
71	Windows Audio	Вручну (Manual)
72	Служба завантаження зображень (WIA) (Windows Image Acquisition (WIA))	Відключено (Disabled)
73	Windows Installer	Вручну (Manual)
74	Інструментарій керування Windows (Windows Management Instrumentation)	Авто (Auto)
75	Розширення драйверів WMI (Windows Management Instrumentation Driver Extension)	Вручну (Manual)
76	Служба часу Windows (Windows Time)	Відключено (Disabled)
77	Бездротове настроювання (Wireless Zero Configuration)	Відключено (Disabled)
78	Адаптер продуктивності WMI (WMI Performance Adapter)	Відключено (Disabled)
79	Робоча станція (Workstation)	Авто (Auto)
80	Центр забезпечення безпеки	Відключено

№ п/п	Назва параметра	Параметр (Установка)
	(Security Center)	(Disabled)
81	Протокол HTTP SSL (HTTP SSL)	Авто (Auto)
82	Служба забезпечення мережі (Network Support)	Авто (Auto)

6 Налаштування реєстру

Параметри налаштовуються за допомогою редактора реєстру.

Параметри наведені в табл. 8.

Таблиця 8

№ п/п	Назва параметра	Subkey Registry Value Entry	Шлях	Format	Зна-чення
1	Відключення автозапуску для всіх дисків (Disable Autorun for all drives)	NoDriveType AutoRun	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\Current Version\Policies\ Explorer\ registry key	DWORD	0xFF
2	Час у секундах перед завершенням пільгового періоду екрана заставки (The time in seconds before the screen saver grace period expires (0 recommended))	ScreenSaver Grace Period	HKEY_LOCAL_MACHINE\SYSTEM\Software\ Microsoft\WindowsNT\CurrentVersion\ Winlogon\ registry key	STRING	0
3	Відсоток заповнення журналу подій безпеки, після якого система починає видавати повідомлення про заповнення (Percentage threshold for the security event logat which the system will generate a warning)	Warning Level	HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services\Eventlog\ Security\registry key	DWORD	90
4	Перевірка бібліотек DLL (Enable Safe DLL search mode (recommended)	SafeDllSearh Mode	HKEY_LOCAL_MACHINE\ SYSTEM\Current ControlSet\Control\SessionManager\ registry key	DWORD	1
5	Відключити автоматичний вхід до системи (Disable Automatic Logon)	AutoAdmin Logon	HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ registry key.	DWORD	0
6	Видалення спільних адміністративних ресурсів (Delete Administrative Shares)	AutoShare Wks	HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Services\Lanman Server\Parameters\ registry key	DWORD	1
7	Сховати комп'ютер у списку перегляду (Hide Computer From	Hidden	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\ registry	DWORD	1

№ п/п	Назва параметра	Subkey Registry Value Entry	Шлях	Format	Зна-чення
	the Browse List)		key.		

7 Файлова система

7.1. Параметри безпеки файлової системи

Параметри налаштовуються за допомогою редактора політики за адресою:
Конфігурація комп'ютера\ Конфігурація Windows\ Параметри безпеки\ Файлова система

Параметри наведені в табл. 9.

Таблиця 9

Папка або файл	Група користувачів	Рекомендований Дозвіл	Застосовуються до	Метод успадку-вання
%AllUsersProfile% (Папка, яка зазвичай містить атрибути робочого столу та профілів усіх користувачів, C:\Documents and Settings\All Users)	Адміністратори	Повний доступ	Папка, підпапки й файли	Поши-рення
	Система	Повний доступ	Папка, підпапки й файли	
	Користувачі	Читання й виконання	Папка, підпапки й файли	
%AllUsersProfile%\Application Data\ Microsoft (Містить дані документів застосувань Майкрософт)	Адміністратори	Повний доступ	Папка, підпапки й файли	Заміна
	Система	Повний доступ	Папка, підпапки й файли	Заміна
	Користувачі	Читання й виконання	Папка, підпапки й файли	
	Досвідчені користувачі	Огляд папок, Виконання файлів, Список вмісту папки, Читання даних	Папка, підпапки й файли	
		Читання атрибутів, Читання додатко-вих атрибутів, Створення файлів, Запис даних, Створення папок, Додавання даних, Запис атрибутів		
%AllUsersProfile%\ ApplicationData\ Microsoft\Crypto\ DSS\Machine	Адміністратори	Повний доступ	Папка, підпапки й файли	Заміна
	Система	Повний доступ	Папка, підпапки й файли	Заміна

Папка або файл	Група користувачів	Рекомендований Дозвіл	Застосовуються до	Метод успадку-вання
Keys	Користувачі	Список вмісту папки,Читання атрибутів, Читання додаткових атрибутів, Створення файлів, Створення папок, Запис атрибутів, Запис додаткових атрибутів, Читання дозволів	Тільки папка	
%AllUsersProfile%\Application Data\ Microsoft\Crypto\ RSA\Machine Keys	Адміністратори	Повний доступ	Папка, підпапки й файли	Заміна
	Система	Повний доступ	Папка, підпапки й файли	Заміна
		Запис атрибутів, Запис додатко-вих атрибутів, Читання дозволів		
%AllUsersProfile%\ ApplicationData\ Microsoft\HTML Help	Адміністратори	Повний доступ	Папка, підпапки й файли	Заміна
	Система	Повний доступ	Папка, підпапки й файли	
	Користувачі	Читання й виконання	Папка, підпапки й файли	
	Досвідчені користувачі	Зміна	Папка, підпапки й файли	
%AllUsersProfile%\Application Data\ Microsoft\Media Index	Адміністратори	Повний доступ	Папка, підпапки й файли	Заміна
	Система	Повний доступ	Папка, підпапки й файли	
	Користувачі	Створення файлів, Створення папок, Запис атрибутів, Запис додаткових атрибутів, Читання дозволів	Тільки папка	
	Користувачі	Запис	Папка, підпапки й файли	
	Користувачі	Читання й виконання	Папка, підпапки й файли	
	Досвідчені користувачі	Огляд папок, Виконання файлів, Список змісту папки, Читання даних	Папка, підпапки й файли	

Папка або файл	Група користувачів	Рекомендований Дозвіл	Застосовуються до	Метод успадкування
		Читання атрибутів, Читання додаткових атрибутів, Створення файлів, Запис даних, Створення папок, Додавання даних, Запис атрибутів, Запис додаткових атрибутів Видалення підпапок і файлів, Видалення, Читання дозволів		
%AllUsersProfile%\ DRM	Ігнорувати			Ігнорувати
%SystemDrive%\ (Диск, на якому встановлена ОС Windows XP, містить важливі файли заванта-ження та налагодження операційної системи)	Адміністратори	Повний доступ	Папка, підпапки й файли	Розповсюдження
	Творець-власник	Повний доступ	Папка, підпапки й файли	
	Система	Повний доступ	Папка, підпапки й файли	
	Користувачі	Читання й виконання	Папка, підпапки й файли	
%SystemDrive% \Documents and Settings (Папка містить профілі користу-вачів та профілі за умовчанням)	Адміністратори	Повний доступ	Папка, підпапки й файли	Розповсюдження
	Система	Повний доступ	Папка, підпапки й файли	
	Користувачі	Читання й виконання	Папка, підпапки й файли	
	Досвідчені користувачі	Читання й виконання	Папка, підпапки й файли	
%SystemDrive%\ Documents and ettings\Default User (Папка містить атрибути робочого столу та профілів користувачів, які входять у систему перші, що використовуються за умовчанням.)	Адміністратори	Повний доступ	Папка, підпапки й файли	Заміна
	Система	Повний доступ	Папка, підпапки й файли	
	Користувачі	Читання й виконання	Папка, підпапки й файли	
	Досвідчені користувачі	Читання й виконання	Папка, підпапки й файли	
%SystemRoot% Installer	Адміністратори	Повний доступ	Папка, підпапки й файли	Заміна
	Система	Повний доступ	Папка, підпапки й файли	
	Користувачі	Читання й виконання	Папка, підпапки й файли	

8 Адміністративні шаблони

8.1 Параметри комп'ютера для Установника Windows

Параметри налаштовуються за допомогою редактора політики за адресою:

Конфігурація комп'ютера\ Адміністративні шаблони\ Компонента Windows\ Установник Windows

Параметри наведені в табл. 10.

Таблиця 10

№ п/п	Назва параметра	Параметр (Установка)
1	Заборонити відкат	Відключено

8.2 Параметри комп'ютера для системи

8.2.1 Параметри комп'ютера у вузлі Система

Параметри налаштовуються за допомогою редактора політики за адресою:
Настроювання комп'ютера\ Адміністративні шаблони\ Система

Параметри наведені в табл. 11.

Таблиця 11

№ п/п	Назва параметра	Параметр (Установка)
1	Відключити автозапуск	Включений -Всі диски
2	Відключити запит на використання Windows Update при пошуку драйверів	Включено

8.2.2 Параметри комп'ютера у вузлі Система\вхід до системи

Параметри налаштовуються за допомогою редактора політики за адресою:
Настроювання комп'ютера\ Адміністративні шаблони\ Система\ вхід у систему

Параметри наведені в табл. 12.

Таблиця 12

№ п/п	Назва параметра	Параметр (Установка)
1	Не відображати вікно “Перше знайомство” при вході в систему	Включений
2	Не обробляти список автозапуска для старих версій	Включений
3	Не обробляти список автозапуска програм, виконуваних один раз	Включений

8.2.3 Параметри комп'ютера у вузлі Система\Групова політика

Параметри налаштовуються за допомогою редактора політики за адресою:
Настроювання комп'ютера\ Адміністративні шаблони\ Система\ Групова політика

Параметри наведені в табл. 13.

Таблиця 13

№ п/п	Назва параметра	Параметр (Установка)
1	Обробка політики настроювання Internet Explorer	Включений
2	Обробка політики реєстру	Включений

8.2.4 Параметри комп'ютера у вузлі Система\Дискові квоти

Параметри налаштовуються за допомогою редактора політики за адресою:
Настроювання комп'ютера\ Адміністративні шаблони\ Система\ Дискові квоти
Параметри наведені в табл. 14.

Таблиця 14

№ п/п	Назва параметра	Параметр (Установка)
1	Включити дискові квоти	Включений
2	Задати межу дискової квоти	Включений
3	Межа квоти за замовчуванням і рівень попередження	Включений
4	Вести журнал навіть при перевищенні межі квоти	Включений
5	Заносити подію перевищення рівня попередження квоти	Включений

8.2.5 Параметри комп'ютера у вузлі Система\ Відновлення системи

Параметри налаштовуються за допомогою редактора політики за адресою:
Настроювання комп'ютера\ Адміністративні шаблони\ Система\ Відновлення системи
Параметри наведені в табл. 15.

Таблиця 15

№ п/п	Назва параметра	Параметр (Установка)
1	Відключити відновлення системи	Не заданий
2	Відключити конфігурацію	Не заданий

8.2.6 Параметри користувача для Панелі керування

Параметри налаштовуються за допомогою редактора політики за адресою:
Конфігурація користувача\ Адміністративні шаблони\ Панель керування\Екран
Параметри наведені в табл. 16.

Таблиця 16

№ п/п	Назва параметра	Параметр (Установка)
1	Використати екранні заставки	Включений
2	Ім'я файлу екранної заставки, що виконує	Включений
3	Використати парольний захист для екранних заставок	Включений
4	Тайм-аут екранної заставки	Включений 600 секунд

8.2.7 Параметри користувача для системи

Відповідні параметри налаштовуються за допомогою редактора політики за адресою: **Конфігурація користувача\ Адміністративні шаблони\ Система\ Провідник**
Параметри наведені в табл. 17.

Таблиця 17

№ п/п	Назва параметра	Параметр (Установка)
1	Видалити можливості запису компакт-дисків	Включений
2	Видалити вкладку Безпека	Включений

8.2.8 Параметри редагування реєстру

Відповідні параметри налаштовуються за допомогою редактора політики за адресою: **Конфігурація користувача\ Адміністративні шаблони\ Система**

Параметри наведені в табл. 18.

Таблиця 18

№ п/п	Назва параметра	Параметр (Установка)
1	Зробити недоступними засіб редагування реєстру	Включений

8.2.9 Параметри користувача у вузлі Система\Управління електроживленням

Відповідні параметри налаштовуються за допомогою редактора політики за адресою: **Конфігурація користувача\Адміністративні шаблони\Система\Керування електроживленням**

Параметри наведені в табл. 19.

Таблиця 19

№ п/п	Назва параметра	Параметр (Установка)
1	Запитувати пароль при виході зі сплячого або режиму, що чекає	Включений

8.2.10 Параметри користувача для Диспетчера вкладень

Відповідні параметри налаштовуються за допомогою редактора політики за адресою: **Конфігурація користувача\ Адміністративні шаблони\ Диспетчер вкладень**

Параметри наведені в табл. 20.

Таблиця 20

№ п/п	Назва параметра	Параметр (Установка)
1	Не зберігати відомості про зону у вкладених файлах	Відключений
2	Сховати можливість для видалення відомостей про зону	Включений
3	Повідомляти антивірусну програму при відкритті вкладень	Включений

9 Налаштування мережевого екрану

Для налаштування мережевого екрану необхідно:
- Перейменувати VPN-з'єднання до системи портового співтовариства на «PPL33-35»;
- створити (або завантажити) файл *tune_XP.bat* та виконати його з правами адміністратора.

Зміст файлу *tune_XP.bat*:

```
@echo off

SET FFPATH=C:\OPCIS\ClientFF.exe
SET FAPATH=C:\OPCIS\ClientFA.exe
SET FCPATH=C:\OPCIS\ClientFC.exe
SET FDPATH=C:\OPCIS\ClientFD.exe
SET UPPATH=C:\OPCIS\Update.exe
SET IFNAME=PPL33-35


netsh firewall set opmode mode=disable interface=%IFNAME%
```

netsh firewall add allowedprogram program=%FAPATH% name="PPL33-35 (Agent)" mode=enable
netsh firewall add allowedprogram program=%FFPATH% name="PPL33-35 (Forwarder)" mode=enable
netsh firewall add allowedprogram program=%FCPATH% name="PPL33-35 (Customs)" mode=enable
netsh firewall add allowedprogram program=%FDPATH% name="PPL33-35 (Dispatcher)" mode=enable
netsh firewall add allowedprogram program=%UPPATH% name="PPL33-35 (Update)" mode=enable

ЦЕНТР ОБРОБКИ ДАНИХ:	**КОРИСТУВАЧ**
Товариство з обмеженою відповідальністю «ППЛ 33-35»	Место для ввода текста.
	Место для ввода текста.

Генеральний директор_____ О.О.Федоров