

## І Н С Т Р У К Ц І Я

з інсталяції та конфігурування параметрів безпеки ОС  
Windows 7 Professional Edition  
Windows 7 Enterprise Edition  
Windows 7 Ultimate Edition

### **Вступ**

Корпорація Microsoft разом з носієм ОС Windows 7 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 7 на АРМ користувачів.

В документі розглядається конфігурування параметрів безпеки операційних систем Microsoft Windows 7.

Значення параметрів безпеки наведені в табл. 1-9. Для параметрів, які несуттєві для безпеки, значення не вказані.

Назви параметрів безпеки, які описані у цьому документі, наведені російською та/або англійською мовами.

### **1 Засоби, які використовуються для конфігурування параметрів безпеки**

Для конфігурування параметрів безпеки застосовуються вбудовані системні компоненти ОС Windows 7 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 учетных записей)**

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

#### **2.1 Політика паролів (Політика паролей)**

Параметри налаштовуються за допомогою редактора політики за адресою:

**Політики учетных записей\ Політика паролей**

Параметри наведені в табл. 1.

Таблица 1

№ п/п	Назва параметра	Параметр (Установка)
1	Вести журнал паролей (Enforce password history)	24 хранимых пароля (24 passwords remembered)
2	Максимальный срок действия пароля (Maximum password age)	31 дня (31 days)
3	Минимальный срок действия пароля	30 дней

№ п/п	Назва параметра	Параметр (Установка)
	(Minimum password age)	(30 days)
4	Минимальная длина пароля (Minimum password lengths) <sup>1</sup>	8
5	Пароль должен отвечать требованиям сложности (Password must meet complexity requirements)	Включен (Enabled)
6	Хранить пароли, используя обратимое шифрование (Store password using reversible encryption)	Отключен (Disabled)

## 2.2 Політика блокування облікового запису (Политика блокировки учетной записи)

Політика блокування облікового запису використовується для блокування облікового запису, якщо протягом заданого проміжку часу реєструється визначена кількість невдалих спроб входу до системи. Кількість спроб і інтервал часу встановлюються за допомогою параметрів політики облікового запису.

Відповідні параметри налаштовуються за допомогою редактора політики за зазначеною адресою:

**Политики учетных записей \ Политика блокировки учетной записи**

Рекомендовані параметри наведені в табл. 2.

Таблица 2

№ п/п	Назва параметра	Параметр (Установка)
1	Время до сброса блокировки (Account lockout duration)	30 минут (30 minutes)
2	Пороговое значение блокировки (Account lockout duration) <sup>2</sup>	10 ошибок входа в систему (10 invalid logon attempts)
3	Продолжительность блокировки учетной записи (Reset account lockout counter after)	30 минут (30 minutes)

Більш детальну інформацію про налаштування параметрів політики облікових записів можна знайти в Windows 7 Security Guide (Руководство по безопасности Windows 7). Microsoft Corporation, 2009.

## 3 Параметри локальної політики (Параметры локальной политики)

До параметрів локальної політики відносять політику аудита, призначення прав користувачів та параметри безпеки.

### 3.1 Політика аудиту (Политика аудита)

За допомогою політики аудита визначаються події безпеки, які заносяться в журнал реєстрації. Адміністратор отримує можливість слідкувати за діями, які **МАЮТЬ ВІДНОШЕННЯ ДО БЕЗПЕКИ**, наприклад доступом до об'єктів, входом (виходом) з системи.

<sup>1</sup> Слід зауважити, що довгі паролі, які складаються з восьми і більше символів, як правило, значно надійніші за короткі, але застосування дуже довгих паролів приводить до збільшення кількості помилок при введенні пароля, збільшенню кількості заблокованих облікових записів і, як наслідок, звернень в службу підтримки користувачів мережі. Крім того, використання дуже довгих паролів може привести до фактичного зниження безпеки, тому що користувачі через боязнь забути пароль вимушені його записувати. Фактичне значення довжини пароля визначається відповідно до політики безпеки організації.

<sup>2</sup> Стандартне граничне значення параметра “Пороговое значение блокировки”, яке рекомендується, дорівнює 50 невдалих спроб входу до системи, але насправді це значення залежить повністю від політики організації. Невелике значення цього параметра підвищує імовірність проведення атаки типу “Відмова від обслуговування” (DoS).

Відповідні параметри налаштовуються за допомогою редактора політики за зазначеною адресою:

**Локальные политики\ Политика аудита**  
Рекомендовані параметри наведені в табл. 3.

Таблица 3

№ п/п	Назва параметра	Параметр (Установка)
1	Аудит входа в систему (Audit account logon events)	Успех, Отказ (Success, Failure)
2	Аудит управления учетными записями (Audit account management)	Успех, Отказ (Success, Failure)
3	Аудит доступа к службе каталогов (Audit directory service access)	Успех, Отказ (Success, Failure)
4	Аудит событий входа в систему (Audit logon events)	Успех, Отказ (Success, Failure)
5	Аудит доступа к объектам (Audit object access)	Успех, Отказ (Success, Failure)
6	Аудит изменения политики (Audit policy change)	Успех, Отказ (Success, Failure)
7	Аудит использования привилегий (Audit privilege use)	Успех, Отказ (Success, Failure)
8	Аудит отслеживания процессов (Audit process tracking)	Успех, Отказ (Success, Failure)
9	Аудит системных событий (Audit system events)	Успех, Отказ (Success, Failure)

### 3.2 Параметры назначения прав пользователей (Параметры назначения прав пользователя)

Параметры назначения прав пользователей позволяют назначить привилегии пользователям и группам.

Відповідні параметри налаштовуються за допомогою редактора політики за зазначеною адресою:

**Локальные политики\ Назначение прав пользователей**

При налаштуванні параметрів безпеки локального об'єкта групової політики комп'ютера, який не є членом домену, значення „Не определено” (Not defined) і „Никто” (No One) не відрізняються та визначають, що нікому користувачу не надаються відповідні привілеї. Обидва значення задаються в редакторі „Локальна політика безпеки” шляхом видалення всіх користувачів зі списку відповідного параметра.

При налаштуванні параметрів безпеки об'єктів групової політики Active Directory домену ці значення мають наступний сенс:

- „Не определено” (Not defined) – визначає, що при формуванні результуючої політики, даний об'єкт групової політики *не впливає* на відповідний параметр політики. Це значення налаштовується шляхом деактивування відповідного параметра інтерфейсу редактора групової політики Active Directory;
- „Никто” (No One) – визначає, що при формуванні результуючої політики, даний об'єкт групової політики *перекриває* значення відповідного параметра попередніх об'єктів шляхом очищення списку користувачів та груп користувачів. Це значення налаштовується шляхом активування параметра без внесення в список користувачів, яким надаються відповідні привілеї, жодного з користувачів або груп користувачів

Параметри наведені в табл. 4.

Таблица 4

№ п/п	Назва параметра	Параметр (Установка)
1	Архивирование файлов и каталогов (Back up files and directories)	Администраторы (Administrators)

<b>№ п/п</b>	<b>Назва параметра</b>	<b>Параметр (Установка)</b>
<b>2</b>	Блокировка страниц в памяти (Lock pages in memory)	Никто (None)
<b>3</b>	Восстановление файлов и каталогов (Restore files and directories)	Администраторы (Administrators)
<b>4</b>	Вход в качестве пакетного задания (Log on as a batch job)	Никто (None)
<b>5</b>	Вход в качестве службы (Log on as a service)	Никто (None)
<b>6</b>	Выполнение задач по обслуживанию томов (Perform volume maintenance tasks)	Администраторы (Administrators)
<b>7</b>	Добавление рабочих станций к домену (Add workstations to domain)	Администраторы (Administrators)
<b>8</b>	Доступ к диспетчеру учетных данных от имени доверенного вызывающего (Access credential Manager as a trusted caller)	Никто (No One)
<b>9</b>	Доступ к компьютеру из сети (Access this computer from the network)	Администраторы (Administrators)
<b>10</b>	Завершение работы системы (Shut down the system)	Администраторы, Пользователи (Administrators, Users)
<b>11</b>	Загрузка и выгрузка драйверов устройств (Load and unload device drivers)	Администраторы (Administrators)
<b>12</b>	Замена маркера уровня процесса (Replace a process level token)	LOCAL SERVICE, NETWORK SERVICE
<b>13</b>	Запретить вход в систему через службу терминалов (Deny logon through Terminal Services)	Гости, АНОНИМНЫЙ ВХОД (Guests, ANONYMUS LOGON)
<b>14</b>	Запретить локальный вход (Deny log on locally)	Гости, АНОНИМНЫЙ ВХОД (Guests, ANONYMUS LOGON)
<b>15</b>	Изменение метки объекта (Modify an object label)	Никто (No One)
<b>16</b>	Изменение параметров среды изготовителя (Modify firmware environment values)	Администраторы (Administrators)
<b>17</b>	Изменение системного времени (Change the system time)	Администраторы, LOCAL SERVICE (Administrators)
<b>18</b>	Изменение часового пояса (Change the time zone)	Администраторы, LOCAL SERVICE (Administrators)
<b>19</b>	Имитация клиента после проверки подлинности (Impersonate a client after authentication)	Администраторы, СЛУЖБА, LOCAL SERVICE, NETWORK SERVICE (Administrators, SERVICE)
<b>20</b>	Локальный вход в систему (Allow log on locally)	Администраторы, Пользователи (Administrators, Users)
<b>21</b>	Настройка квот памяти для процесса (Adjust memory quotas to a process)	Администраторы, СЛУЖБА (Administrators), LOCAL SERVICE,

<b>№ п/п</b>	<b>Назва параметра</b>	<b>Параметр (Установка)</b>
		NETWORK SERVICE
22	Обход перекрестной проверки (Bypass traverse checking)	Прошедшие проверку, LOCAL SERVICE, NETWORK SERVICE
23	Отказ в доступе к компьютеру из сети (Deny access to this computer from the network)	Гости, АНОНИМНЫЙ ВХОД (Guests, ANONYMUS LOGON)
24	Отказ во входе в качестве пакетного задания (Deny logon as a batch job)	Гости, АНОНИМНЫЙ ВХОД (Guests, ANONYMUS LOGON)
25	Отказ во входе в качестве службы (Deny log on as a service)	Не определено (No defined)
26	Отключение компьютера от стыковочного узла (Remove computer from docking station)	Администраторы (Administrators)
27	Отладка программ (Debug programs)	Никто (No one)
28	Принудительное удаленное завершение работы (Force shutdown from a remote system)	Администраторы (Administrators)
29	Профилирование одного процесса (Profile single process)	Администраторы (Administrators)
30	Профилирование производительности системы (Profile system performance)	Администраторы (Administrators)
31	Работа в режиме операционной системы (Act as part of the operating system)	Никто (No One)
32	Разрешать вход в систему через службу удаленных рабочих столов (Allow logon through Remote Desktop Services)	Администраторы, (Administrators)
33	Разрешения доверия к учетным записям при делегировании (Enable computer and user accounts to be trusted for delegation)	Не определено (Not defined)
34	Синхронизация данных службы каталогов (Synchronize directory service data)	Никто (No One)
35	Смена владельцев файлов и других объектов (Take ownership of files or other objects)	Администраторы (Administrators)
36	Создание аудитов безопасности (Generate security audits)	LOCAL SERVICE, NETWORK SERVICE
37	Создание глобальных объектов (Create global objects)	Администраторы (Administrators), LOCAL SERVICE, NETWORK SERVICE
38	Создание маркерного объекта (Create a token object)	Никто (No one)
39	Создание постоянных общих объектов (Create permanent shared objects)	Никто (No one)
40	Создание символических ссылок (Create symbolic links)	Никто (No one)
41	Создание файла подкачки (Create a pagefile)	Администраторы (Administrators)
42	Увеличение приоритета выполнения (Increase scheduling priority)	Администраторы (Administrators)
43	Увеличение рабочего набора процесса	Администраторы, LOCAL

№ п/п	Назва параметра	Параметр (Установка)
	(Increase a process working set)	SERVICE (Administrators)
44	Управление аудитом и журналом безопасности (Manage auditing and security log)	Администраторы (Administrators)

### 3.3 Параметры безопасности (Параметры безопасности)

Параметры безопасности позволяют задаться или отключить ряд функций например, цифровой подписи данных, имя учетных записей администратора и гостя, доступ к дисководом гибких и компакт-дисков, установку драйверов, уведомления при входе в систему и т.д.

Соответствующие параметры настраиваются с помощью редактора политики за заданной адресом:

**Конфигурация компьютера\ Конфигурация Windows\ Параметры безопасности\ Локальные политики\ Параметры безопасности**

Параметры приведены в табл. 5.

Таблица 5

№ п/п	Назва параметра	Параметр (Установка)
1	Учетные записи: состояние учетной записи «Администратор» (Accounts: Administrator account status)	Отключен (Disabled)
2	Учетные записи: состояние учетной записи «Гость» (Accounts: Guest account status)	Отключен (Disabled)
3	Учетные записи: разрешить использование пустых паролей только при консольном входе (Accounts: Limit local account use of blank passwords to console logon only)	Включен (Enabled)
4	Учетные записи: Переименование учетной записи администратора (Accounts: Rename administrator account)	Рекомендуется <sup>3</sup> (Recommend)
5	Учетные записи: Переименование учетной записи гостя (Accounts: Rename guest account)	Рекомендуется <sup>4</sup> (Recommend)
6	Аудит: Аудит доступа глобальных системных объектов (Audit: Audit the access of global system objects)	Отключен (Disabled)
7	Аудит: Аудит прав на архивацию и восстановление (Audit: Audit the use of Backup and Restore privilege)	Отключен (Disabled)
8	Аудит: Немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности (Audit: Shut down system immediately if unable to log security audits)	Включен (Enabled)
9	Аудит: принудительно переопределяет параметры подкатегории политики аудита параметров категории политики аудита (Audit: Force audit policy subcategory settings to override audit policy category settings)	Включен (Enabled)

<sup>3</sup> Корпорация Microsoft рекомендует выбрать для встроенной учетной записи «Администратор» другое имя и в дальнейшем уникализировать использование имен с явно выраженными знаками административных полномочий учетных записей

<sup>4</sup> Майкрософт также рекомендует переименовать этот учетный записи так, чтобы новое имя не отображало назначения этого учетного записи. Даже при отключении этого учетного записи (рекомендуется), в целях дополнительной безопасности переименуется в то, что она переименована.

<b>№ п/п</b>	<b>Назва параметра</b>	<b>Параметр (Установка)</b>
<b>10</b>	Устройства: Разрешать отстыковку без входа в систему (Devices: Allow undock without having to log on)	Отключен (Disabled)
<b>11</b>	Устройства: Разрешить форматирование и извлечение съемных носителей (Devices: Allowed format and eject removable media)	Администраторы (Administrators)
<b>12</b>	Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям (Devices: Restrict CD-ROM access to locally logged-on user only) <sup>5</sup>	Отключен (Disabled)
<b>13</b>	Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям (Devices: Restrict floppy access to locally logged-on user only)	Отключен (Disabled)
<b>14</b>	Устройства: запретить пользователям установку драйверов принтера (Devices: Prevent users from installing printer drivers)	Включен (Enabled)
<b>15</b>	Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию (Domain controller: Allow server operators to schedule tasks)	Отключен (Disabled)
<b>16</b>	Контроллер домена: Требование цифровой подписи для LDAP сервера (Domain controller: LDAP server signing requirements)	Нет
<b>17</b>	Контроллер домена: Запретить изменение пароля учетных записей компьютера (Domain controller: Refuse machine account password changes)	Отключен (Disabled)
<b>18</b>	Член домена: Всегда требуется цифровая подпись или шифрование потока данных безопасного канала (Domain member: Digitally encrypt or sign secure channel data (always))	Включен (Enabled)
<b>19</b>	Член домена: Шифрование данных безопасного канала, когда это возможно (Domain member: Digitally encrypt secure channel data (when possible))	Включен (Enabled)
<b>20</b>	Член домена: Максимальный срок действия пароля учетных записей компьютера (Domain member: Maximum machine account password age)	30 дней (30 days)
<b>21</b>	Член домена: Цифровая подпись данных безопасного канала, когда это возможно (Domain member: Digitally sign secure channel data (when possible))	Включен (Enabled)
<b>22</b>	Член домена: Отключить изменение пароля учетных записей компьютера (Domain member: Disable machine account password changes)	Отключен (Disabled)
<b>23</b>	Член домена: требовать стойкий ключа сеанса (Windows 2000 или выше)	Включен (Enabled)

<sup>5</sup> Якщо не планується надання користувачам права встановлювати програмне забезпечення на клієнтських машинах, потрібно встановлювати для даного параметра значення "Включен". Те ж саме стосується параметра "Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям".

№ п/п	Назва параметра	Параметр (Установка)
	(Domain member: Require strong (Windows 2000 or later) session key)	
24	Интерактивный вход в систему: Не отображать последнее имя пользователя (Interactive logon: Do not display last user name)	Включен (Enabled)
25	Интерактивный вход в систему: Не требовать нажатия CTRL+ALT+DEL (Interactive logon: Do not require CTRL+ALT+DEL)	Отключен (Disabled)
26	Интерактивный вход в систему: Текст сообщения для пользователей при входе в систему (Interactive logon: Message text for users attempting to log on)	Вхід тільки для авторизованих користувачів. Особи, які здійснюють спроби несанкціонованого доступу, переслідуються згідно із законом
27	Интерактивный вход в систему: Заголовок сообщения для пользователей при входе в систему (Interactive logon: Message title for users attempting to log on)	ПРОДОВЖЕННЯ СПРОБ БЕЗ НАЛЕЖНОЇ АВТОРИЗАЦІЇ Є ЗЛОЧИНОМ
28	Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) (Interactive logon: Number of previous logons to cache (in case domain controller is not available))	0
29	Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее (Interactive logon: Prompt user to change password before expiration)	5 дней (5 days)
30	Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера (Interactive logon: Require Domain controller authentication to unlock workstation)	Включен (Enabled)
31	Интерактивный вход в систему: требовать смарт-карту (Interactive logon: Smart card removal behavior)	Отключен (Disabled)
32	Интерактивный вход в систему: поведение при извлечении смарт карты (Interactive Logon: Smart card removal behavior)	Блокировка рабочей станции
33	Интерактивный вход в систему: отображать сведения о пользователе если сеанс заблокирован (Interactive Logon: Display user name when workstation locked)	Не отображать сведения о пользователе
34	Клиент сети Microsoft: использовать цифровую подпись (всегда) (Microsoft network client: Digitally sign communications (always))	Включен (Enabled)
35	Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера) (Microsoft network client: Digitally sign communications (if server agrees))	Включен (Enabled)



№ п/п	Назва параметра	Параметр (Установка)
36	Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам (Microsoft network client: Send unencrypted password to third-party SMB servers)	Отключен (Disabled)
37	Сервер сети Microsoft: Время бездействия до приостановки сеанса (Microsoft network server: Amount of idle time required before suspending session)	10 минут (10 minutes)
38	Сервер сети Microsoft: Использовать цифровую подпись (всегда) (Microsoft network server: Digitally sign communications(always))	Включен (Enabled)
39	Сервер сети Microsoft: Использовать цифровую подпись (с согласия клиента) (Microsoft network server: Digitally sign communications (if client agrees))	Включен (Enabled)
40	Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа (Microsoft network server: Disconnect clients when logon hours expire )	Включен (Enabled)
41	Доступ к сети: Разрешить трансляцию анонимного SID в имя (Network access: Allow anonymous SID/Name translation)	Отключен (Disabled)
42	Сетевой доступ: Не разрешать перечисление учетных записей SAM анонимными пользователями (Network access: Do not allow anonymous enumeration of SAM accounts)	Включен (Enabled)
43	Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями (Network access: Do not allow anonymous enumeration of SAM accounts and shares)	Включен (Enabled)
44	Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности	Включен (Enabled)
45	Сетевой доступ: Разрешать применение разрешений «Для всех» к анонимным пользователям (Network access: Let Everyone permissions apply to anonymous users)	Отключен (Disabled)
46	Сетевой доступ: Разрешать анонимный доступ к именованным каналам (Network access: Named Pipes that can be accessed anonymously)	Ни для кого (No one)
47	Сетевой доступ: Разрешать анонимный доступ к общим ресурсам (Network access: (Shares that can be accessed anonymously))	Ни для кого (No one)
48	Сетевой доступ: удаленно доступные пути реестра (Network access: Remotely accessible registry paths)	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

№ п/п	Назва параметра	Параметр (Установка)
49	Сетевой доступ: удаленно доступные пути и вложенные пути реестра (Network access: Remotely accessible registry paths and sub-paths)	Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog
50	Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей (Network access: Sharing and security model for local accounts)	Обычная – локальные пользователи удостоверяются как они сами (Classic – local users authenticate as themselves)
51	Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам (Network access: Restrict anonymous access to Named Pipes and Shares)	Включен (Enabled)
52	Сетевая безопасность: не хранить хеш - значений LAN Manager при следующей смене пароля (Network security: do not store LAN Manager hash value on next password change )	Включен (Enabled)
53	Сетевая безопасность: принудительный вывод из сеанса по истечении допустимых часов работы (Network security: Force logoff when logon hours expire)	Включен (Enabled)
54	Сетевая безопасность: уровень проверки подлинности LAN Manager (Network security: LAN Manager authentication level )	NTLMv2 ответ, отказывать LM и NTLM (Send NTLMv2 response only\refuse LM and NTLM)
55	Сетевая безопасность: Требование цифровой подписи для LDAP клиента (Network security: LDAP client signing requirements)	Согласование цифровой подписи (Require signature)
56	Сетевая безопасность: Минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая	Требовать сеансовую безопасность NTLMv2,

№ п/п	Назва параметра	Параметр (Установка)
	безопасность RPC) (Network security: Minimum session security for NTLM SSP based (including secure RPC) clients)	Требовать 128-битное шифрование (Require NTLMv2 session security, Require 128 bit Encryption)
57	Сетевая безопасность: Минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасность RPC) (Network security: Minimum session security for NTLM SSP based (including secure RPC)servers)	Требовать сеансовую безопасность NTLMv2, Требовать 128-битное шифрование (Require NTLMv2 session security, Require 128 bit Encryption)
58	Сетевая безопасность: настройка типов шифрования, разрешенных Kerberos	DES_CBC_CRC DES_CBC_MD5 RC4_HMAC_MD5 AES128_HMAC_SHA1 AES256_HMAC_SHA1 Будущие типы шифрования
59	Сетевая безопасность: ограничения NTLM: аудит входящего трафика NTLM	Не определено (Not defined)
60	Сетевая безопасность: ограничения NTLM: аудит проверки подлинности NTLM в этом домене	Не определено (Not defined)
61	Сетевая безопасность: ограничения NTLM: входящий трафик NTLM	Не определено (Not defined)
62	Сетевая безопасность: ограничения NTLM: добавить исключения для серверов в этом домене	Не определено (Not defined)
63	Сетевая безопасность: ограничения NTLM: добавить удаленные серверы в исключения проверки подлинности NTLM	Не определено (Not defined)
64	Сетевая безопасность: ограничения NTLM: исходящий трафик NTLM к удаленным серверам	Не определено (Not defined)
65	Сетевая безопасность: ограничения NTLM: проверка подлинности NTLM в этом домене	Не определено (Not defined)
66	Сетевая безопасность: разрешить LocalSystem использовать нулевые сеансы	Не определено (Not defined)
67	Сетевая безопасность: разрешить использование сетевых удостоверений в запросах проверки подлинности PKU2U к этому компьютеру	Отключен (Disabled)
68	Сетевая безопасность: разрешить учетной записи локальной системы использовать удостоверение компьютера для NTLM	Не определено (Not defined)
69	Консоль восстановления: Разрешить Автоматический вход администратора (Recovery console: Allow automatic administrative logon)	Отключен (Disabled)

№ п/п	Назва параметра	Параметр (Установка)
70	Консоль восстановления: Разрешить копирование дискет и доступ ко всем дискам и папкам Администратора (Recovery console: Allow floppy copy and access to all drives and all folders )	Отключен (Disabled)
71	Завершение работы: разрешить завершение работы системы без выполнения входа в систему (Shutdown: Allow system to be shutdown without having to log on)	Отключен (Disabled)
72	Завершение работы: Очистка файла подкачки виртуальной памяти (Shutdown: Clear virtual memory pagefile)	Включен (Enabled)
73	Системная криптография: Использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания (System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing)	Отключен (Disabled)
74	Системная криптография: обязательное применение сильной защиты ключей пользователей, хранящихся на компьютере (System cryptography: Force strong key protection for user keys stored on the computer)	Пользователь должен вводить пароль при каждом использовании ключа.
75	Системные объекты: учитывать регистр для подсистем, отличных от Windows (System objects: Require case insensitivity for non-Windows subsystems)	Включен (Enabled)
76	Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (System objects: Strengthen default permissions of internal system objects (for example, Symbolic Links))	Включен (Enabled)
77	DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)	Не определено (Not defined)
78	DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)	Не определено (Not defined)
79	Контроль учетных записей: все администраторы работают в режиме одобрения администратором (User Account Control: Run all administrators in Admin Approval Mode)	Отключен (Disabled)
80	Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав (User Account Control: Detect application installations and prompt for elevation)	Включен (Enabled)
81	Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав (User Account Control: Switch to the secure desktop when prompting for elevation)	Отключен (Disabled)
82	Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором	Запрос учетных данных

№ п/п	Назва параметра	Параметр (Установка)
	(User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode)	
83	Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей (User Account Control: Behavior of the elevation prompt for standard users)	Запрос учетных данных
84	Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах (User Account Control: Only elevate UIAccess applications that are installed in secure locations)	Включен (Enabled)
85	Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов (User Account Control: Only elevate executables that are signed and validated)	Отключен (Disabled)
86	Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя (User Account Control: Virtualize file and registry write failures to per-user locations)	Включен (Enabled)
87	Контроль учетных записей: разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол (User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop)	Отключен (Disabled)
88	Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора (User Account Control: Admin Approval Mode for the Built-in Administrator account)	Отключен (Disabled)
89	Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ (System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies)	Отключен (Disabled)
90	Параметры системы: необязательные подсистемы (System settings: Optional subsystems)	POSIX
91	Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-службы конечного объекта	Принимать, если предоставлено клиентом

Більш детальну інформацію про налаштування параметрів локальної політики можна знайти в наведених джерелах:

- 1) Windows 7 Security Guide (Руководство по безопасности Windows 7). Microsoft Corporation, 2009
- 2) <http://go.microsoft.com/fwlink/?LinkId=144505>.

#### 4 Журнал подій (Журнал событий)

Параметри журналу подій використовуються для організації запису системних подій. В контейнері “Журнал событий” групової політики задаються атрибути журналів, пов’язаних з застосуваннями, безпекою і системними подіями, такі як максимальний розмір журналу, права доступу до кожного журналу, а також тривалість та способи збереження.

#### 4.1 Параметри безпеки журналу подій (Параметры безопасности журнала событий)

Відповідні параметри налаштовуються за допомогою редактора політики за зазначеною адресою:

**Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Журнал событий**

Параметри наведені в табл. 6.

Таблиця 6

№ п/п	Назва параметра	Параметр (Установка)
1	Запретить доступ локальной группы гостей к журналу приложений (Prevent local guests group from accessing application log)	Включен (Enabled)
2	Запретить доступ локальной группы гостей к журналу безопасности (Prevent local guests group from accessing security log)	Включен (Enabled)
3	Запретить доступ локальной группы гостей к системному журналу (Prevent local guests group from accessing system log)	Включен (Enabled)
4	Максимальный размер журнала приложений (Maximum application log size)	32 768 Кбайт 32 768 KB
5	Максимальный размер журнала безопасности (Maximum security log size)	81 920 Кбайт 81 920 KB
6	Максимальный размер системного журнала (Maximum system log size)	32 768 Кбайт 32 768 KB
7	Метод сохранения событий в журнале приложений (Retention method for application log)	Затирать старые события по необходимости (As Needed)
8	Метод сохранения событий в журнале безопасности (Retention method for security log)	Затирать старые события по необходимости (As Needed)
9	Метод сохранения событий в системном журнале (Retention method for system log)	Затирать старые события по необходимости (As Needed)
10	Сохранять события в журнале приложений (дней) (Retention method for application log)	Не определено (Not defined)
11	Сохранять события в журнале безопасности (дней) (Retention method for security log)	Не определено (Not defined)
12	Сохранять события в системном журнале (дней) (Retention method for system log) <sup>1</sup>	Не определено (Not defined)

#### 5 Системні служби (Системные службы)

### 5.1 Параметры наладки системных служб для компьютеров (Параметры настройки системных служб для компьютеров)

Відповідні параметри налаштовуються за допомогою редактора політики за зазначеною адресою:

**Конфигурация компьютера\ Конфигурация Windows\ Параметры безопасности\ Системные службы**

Параметри наведені в табл. 7.

Таблица 7

№ п/п	Назва параметра	Параметр (Установка)
1.	BranchCache	Не определено
2.	DHCP-клиент	Автоматический
3.	DNS-клиент	Не определено
4.	KtmRm для координатора распределенных транзакций	Не определено
5.	Microsoft .NET Framework NGEN v2.0.50727_X86	Не определено
6.	Microsoft .NET Framework NGEN v4.0.30319_X86	Не определено
7.	Microsoft .NET Framework NGEN v2.0.50727_X64	Не определено
8.	Microsoft .NET Framework NGEN v4.0.30319_X64	Не определено
9.	Parental Controls	Не определено
10.	Plug-and-Play	Автоматический
11.	Quality Windows Audio Video Experience	Не определено
12.	Superfetch	Не определено
13.	Windows Audio	Не определено
14.	Windows CardSpace	Не определено
15.	Windows Driver Foundation - User-mode Driver Framework	Не определено
16.	Windows Search	Не определено
17.	WMI Performance Adapter	Не определено
18.	Автонастройка WWAN	Не определено
19.	Автономные файлы	Не определено
20.	Агент защиты сетевого доступа	Вручную
21.	Агент политики IPsec	Вручную
22.	Адаптивная регулировка яркости	Не определено
23.	Архивация Windows	Вручную
24.	Биометрическая служба Windows	Не определено
25.	Брандмауэр Windows	Автоматический
26.	Браузер компьютеров	Запрещен
27.	Веб-клиент	Вручную
28.	Виртуальный диск	Вручную
29.	Вспомогательная служба IP	Вручную
30.	Вторичный вход в систему	Вручную
31.	Группировка сетевых участников	Не определено
32.	Дефрагментация диска	Вручную
33.	Диспетчер Автоматических подключений удаленного доступа	Вручную
34.	Диспетчер печати	Автоматический
35.	Диспетчер подключений удаленного доступа	Автоматический
36.	Диспетчер сеансов диспетчера окон рабочего стола	Автоматический
37.	Диспетчер удостоверения сетевых участников	Автоматический
38.	Диспетчер учетных данных	Вручную
39.	Диспетчер учетных записей безопасности	Автоматический
40.	Доступ к HID-устройствам	Вручную
41.	Журнал событий Windows	Автоматический
42.	Журналы и оповещения производительности	Вручную

<b>№ п/п</b>	<b>Назва параметра</b>	<b>Параметр (Установка)</b>
43	Защита программного обеспечения	Автоматический
44	Защитник Windows	Автоматический
45	Защищенное хранилище	Автоматический
46	Изоляция ключей CNG	Не определено
47	Инструментарий управления Windows	Не определено
48	Информация о совместимости приложений	Вручную
49	Клиент групповой политики	Автоматический
50	Клиент отслеживания изменившихся связей	Автоматический
51	Координатор распределенных транзакций	Автоматический
52	Кэш шрифтов Windows Presentation Foundation 3.0.0.0	Не определено
53	Ловушка SNMP	Вручную
54	Локатор удаленного вызова процедур (RPC)	Вручную
55	Маршрутизация и удаленный доступ	Запрещен
56	Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности	Автоматический
57	Модуль запуска процессов DCOM-сервера	Автоматический
58	Модуль поддержки NetBIOS через TCP/IP	Автоматический
59	Настройка сервера удаленных рабочих столов	Вручную
60	Немедленные подключения Windows - регистратор настройки	Вручную
61	Обнаружение SSDP	Запрещен
62	Обнаружение интерактивных служб	Вручную
63	Общий доступ к подключению к Интернету (ICS)	Запрещен
64	Определение оборудования оболочки	Автоматический
65	Основные службы доверенного платформенного модуля	Вручную
66	Перенаправитель портов пользовательского режима служб удаленных рабочих столов	Вручную
67	Перечислитель IP-шин PnP-X	Запрещен
68	Питание	Автоматический
69	Планировщик заданий	Автоматический
70	Планировщик классов мультимедиа	Вручную
71	Поддержка элемента панели управления "Отчеты о проблемах и их решениях"	Вручную
72	Политика удаления смарт-карт	Вручную
73	Поставщик домашней группы	Вручную
74	Проводная автонастройка	Вручную
75	Программный поставщик теневого копирования (Microsoft)	Автоматический
76	Прослушиватель домашней группы	Не определено
77	Протокол PNRP	Не определено
78	Публикация ресурсов обнаружения функции	Вручную
79	Рабочая станция	Автоматический
80	Распространение сертификата	Вручную
81	Расширяемый протокол проверки подлинности (EAP)	Вручную
82	Сборщик событий Windows	Вручную
83	Сведения о приложении	Вручную
84	Сервер	Автоматический
85	Сервер упорядочения потоков	Вручную
86	Сетевой вход в систему	Автоматический
87	Сетевые подключения	Вручную



<b>№ п/п</b>	<b>Назва параметра</b>	<b>Параметр (Установка)</b>
88	Система событий COM+	Автоматический
89	Системное приложение COM+	Вручную
90	Служба SSTP	Вручную
91	Служба автоматического обнаружения веб-прокси WinHTTP	Вручную
92	Служба автонастройки WLAN	Автоматический
93	Служба базовой фильтрации	Автоматический
94	Служба ввода планшетного ПК	Вручную
95	Служба времени Windows	Автоматический
96	Служба загрузки изображений Windows (WIA)	Автоматический
97	Служба инициатора Майкрософт iSCSI	Вручную
98	Служба интерфейса сохранения сети	Вручную
99	Служба кэша шрифтов Windows	Автоматический
10	Служба медиаприставки Media Center	Вручную
10	Служба модуля архивации на уровне блоков	Автоматический
10	Служба общего доступа к портам Net.Tcp	Запрещен
10	Служба общих сетевых ресурсов проигрывателя Windows Media	Вручную
10	Служба перечислителя переносных устройств	Вручную
10	Служба планировщика Windows Media Center	Вручную
10	Служба поддержки Bluetooth	Запрещен
10	Служба политики диагностики	Автоматический
10	Служба помощника по совместимости программ	Автоматический
10	Служба профилей пользователей	Автоматический
11	Служба публикации имен компьютеров PNRP	Вручную
11	Служба регистрации ошибок Windows	Вручную
11	Служба ресивера Windows Media Center	Вручную
11	Служба сведений о подключенных сетях	Автоматический
11	Служба списка сетей	Вручную
11	Служба технологий активации Windows	Вручную
11	Служба уведомления SPP	Вручную
11	Служба уведомления о системных событиях	Автоматический
11	Служба удаленного управления Windows (WS-Management)	Автоматический
11	Служба хранилища	Вручную
12	Служба шифрования дисков BitLocker	Вручную
12	Служба шлюза уровня приложения	Вручную
12	Службы криптографии	Автоматический
12	Службы удаленных рабочих столов	Вручную
12	Смарт-карта	Вручную
12	Сопоставитель конечных точек RPC	Автоматический
12	Средство построения конечных точек Windows Audio	Вручную
12	Телефония	Вручную
12	Темы	Не определено
12	Теневое копирование тома	Вручную
13	Тополог канального уровня	Вручную
13	Удаленный вызов процедур (RPC)	Автоматический
13	Удаленный реестр	Вручную
13	Удостоверение приложения	Автоматический
13	Узел системы диагностики	Вручную
13	Узел службы диагностики	Вручную
13	Узел универсальных PNP-устройств	Вручную

№ п/п	Назва параметра	Параметр (Установка)
13	Управление приложениями	Вручную
13	Управление сертификатами и ключом работоспособности	Вручную
13	Установщик ActiveX (AxInstSV)	Вручную
14	Установщик Windows	Вручную
14	Установщик модулей Windows	Вручную
14	Факс	Вручную
14	Фоновая интеллектуальная служба передачи (BITS)	Автоматический
14	Хост поставщика функции обнаружения	Не определено
14	Цветовая система Windows (WCS)	Не определено
14	Центр обеспечения безопасности	Автоматический
14	Центр обновления Windows	Вручную
14	Шифрованная файловая система (EFS)	Вручную

### 6 Налаштування реєстру (Настройка реестра)

В даному підрозділі наведені значення ключів реєстру, які мають відношення до безпеки та можуть бути налаштовані за допомогою редактора політики.

Параметри наведені в табл. 8.

Таблиця 8

№ п/п	Назва параметра	Subkey Registry Value Entry	Шлях	Format	Значення
1	Отключить Автоматический вход в систему (Disable Automatic Logon)	AutoAdminLogon	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\	Параметр DWORD (32 бита) REG_DWORD	0
2	Уровень защиты маршрутизации IP-источника (DisableIPSourceRouting)	DisableIPSourceRouting	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\	Параметр DWORD (32 бита) REG_DWORD	0
3	Разрешить автоматическое обнаружение нерабочих сетевых шлюзов (может привести к отказу в обслуживании) (EnableDeadGWDetect)	DeadGWDetectDefault	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\	Параметр DWORD (32 бита) REG_DWORD	0
4	Разрешить переадресацию ICMP для переопределения созданных маршрутов OSPF (EnableICMPRedirect)	EnableICMPRedirect	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\	Параметр DWORD (32 бита) REG_DWORD	0 <sup>6</sup>
5	Отключить автозапуск для всех дисков	NoDriveTypeAutoRun	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Window	Параметр DWORD	FF

<sup>6</sup> Значений параметр може бути змінено на «Не определен» у випадку використання протоколу маршрутизації OSPF

№ п/п	Назва параметра	Subkey Registry Value Entry	Шлях	Format	Значення
	(NoDriveTypeAutoRun)		s\CurrentVersion\Policies\Explorer\	(32 бита) REG_DWORD	
6	Разрешить компьютеру не создавать имена файлов в формате 8.3 (рекомендуется) (NtfsDisable8dot3NameCreation)	NtfsDisable8dot3NameCreation	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\	Параметр DWORD (32 бита) REG_DWORD	1

## 7 Файлова система (Файловая система)

Стандартні повноваження доступу для файлової системи NTFS підходять для більшості організацій. Параметри налаштування файлової системи, які описані в цьому підрозділі, рекомендується використовувати в першу чергу для систем з високим рівнем безпеки.

### 7.1. Параметри безпеки файлової системи (Параметры безопасности файловой системы)

Відповідні параметри налаштовуються за допомогою редактора політики за зазначеною адресою:

**Конфигурация компьютера\ Конфигурация Windows\ Параметры безопасности\ Файловая система**

Рекомендовані параметри наведені в табл. 9.

Таблица 9

Папка або файл (Папка или файл)	Група користувачів (Группа пользователей)	Рекомендований Дозвіл (Рекомендуемое Разрешение)	Застосовуються до (Применяются к)	Метод Успадкування (Метод наследования)
C:\Users\ (Папка, яка містить атрибути робочого столу та профілів усіх користувачів, зазвичай)	Администраторы	Полный доступ	Для этой папки, ее подпапок и фалов	Распространение
	Система	Полный доступ	Для этой папки, ее подпапок и фалов	
	Пользователи	Чтение и выполнение	Для этой папки, ее подпапок и фалов	
C:\Program Data\Microsoft\ (Містить дані документів застосувань Майкрософт)	Администраторы	Полный доступ	Для этой папки, ее подпапок и фалов	Замена
	Система	Полный доступ	Для этой папки, ее подпапок и фалов	
	Пользователи	Чтение и выполнение	Для этой папки, ее подпапок и фалов	
%SystemDrive%\br/>(Диск, на якому	Администраторы	Полный доступ	Для этой папки, ее подпапок и фалов	Распространение

Папка або файл (Папка или файл)	Група користувачів (Группа пользователей)	Рекомендований Дозвіл (Рекомендуемое Разрешение)	Застосовуються до (Применяются к)	Метод Успадкування (Метод наследования)
встановлена ОС Windows, містить важливі файли завантаження та налагодження операційної системи)	Прошедшие проверку	Траверс папок/выполнение файлов, содержание папки/чтение данных, чтение атрибутов, чтение дополнительных атрибутов, создание файлов/запись данных, создание папок/дозапись данных, запись атрибутов, запись дополнительных атрибутов, удаление, чтение разрешений	Только для папок и файлов	
		Создание папок/дозапись данных	Только для этой папка	
	Система	Полный доступ	Для этой папки, ее подпапок и фалов	
	Пользователи	Чтение и выполнение	Для этой папки, ее подпапок и фалов	
%PROGRAMDAT A%\Microsoft\Win dows\DRM	Все	Траверс папок/выполнение файлов, содержание папки/чтение данных, чтение атрибутов, чтение дополнительных атрибутов, создание файлов/запись данных, создание папок/дозапись данных, запись атрибутов, запись дополнительных атрибутов, удаление папок и файлов, чтение разрешений, смена разрешений, смена владельца	Только для этой папки	
		Полный доступ	Только для подпапок и файлов	

Папка або файл (Папка или файл)	Група користувачів (Група пользователей)	Рекомендований Дозвіл (Рекомендуемое Разрешение)	Застосовуються до (Применяются к)	Метод Успадкування (Метод наследования)
	Система	Полный доступ	Только для этой папки	
	Гость	Все Запрещен	Для этой папки, ее подпапок и файлов	
	Гости	Все Запрещен	Для этой папки, ее подпапок и файлов	
		Полный доступ	Только для подпапок и файлов	
	Система	Полный доступ	Только для этой папки	
	Гость	Все Запрещен	Для этой папки, ее подпапок и файлов	
	Гости	Все Запрещен	Для этой папки, ее подпапок и файлов	
C:\windows\system32\appmgmt	Администраторы	Полный доступ	Для этой папки, ее подпапок и файлов	
	Все	Полный доступ	Только для этой папки	
	Система	Полный доступ	Для этой папки, ее подпапок и файлов	
%Systemroot%\config\default	Администраторы	Полный доступ	Для этого файла	
	Система	Полный доступ	Для этого файла	
%Systemroot%\config\sam	Администраторы	Полный доступ	Для этого файла	
	Система	Полный доступ	Для этого файла	
%Systemroot%\config\security	Администраторы	Полный доступ	Для этого файла	
	Система	Полный доступ	Для этого файла	
%Systemroot%\config\software	Администраторы	Полный доступ	Для этого файла	
	Система	Полный доступ	Для этого файла	
%Systemroot%\config\system	Администраторы	Полный доступ	Для этого файла	
	Система	Полный доступ	Для этого файла	

## 8 Налаштування мережевого екрану

Для налаштування мережевого екрану необхідно створити (або завантажити) файл *tune.bat* та виконати його з правами адміністратора. Після виконання командного файлу EOM автоматично перезавантажиться.

Зміст файлу *tune.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 SMC=HKLM\Software\Policies\Microsoft\WindowsFirewall
```

```
reg add %SMC% /f
reg add %SMC%\PrivateProfile /f
reg add %SMC%\PrivateProfile /v DisableStealthMode /t REG_DWORD /d 1 /f
reg add %SMC%\PublicProfile /f
reg add %SMC%\PublicProfile /v DisableStealthMode /t REG_DWORD /d 1 /f
reg add %SMC%\StandardProfile /f
reg add %SMC%\StandardProfile /v DisableStealthMode /t REG_DWORD /d 1 /f
```

```
netsh advfirewall firewall add rule name="PPL33-35 (Agent)" dir=in action=allow
program=%FAPATH%
netsh advfirewall firewall add rule name="PPL33-35 (Agent)" dir=out action=allow
program=%FAPATH%
```

```
netsh advfirewall firewall add rule name="PPL33-35 (Customs)" dir=in action=allow
program=%FCPATH%
netsh advfirewall firewall add rule name="PPL33-35 (Customs)" dir=out action=allow
program=%FCPATH%
```

```
netsh advfirewall firewall add rule name="PPL33-35 (Forwarder)" dir=in action=allow
program=%FFPATH%
netsh advfirewall firewall add rule name="PPL33-35 (Forwarder)" dir=out action=allow
program=%FFPATH%
```

```
netsh advfirewall firewall add rule name="PPL33-35 (Dispatcher)" dir=in action=allow
program=%FDPATH%
netsh advfirewall firewall add rule name="PPL33-35 (Dispatcher)" dir=out action=allow
program=%FDPATH%
```

```
netsh advfirewall firewall add rule name="PPL33-35 (Update)" dir=in action=allow
program=%UPPATH%
netsh advfirewall firewall add rule name="PPL33-35 (Update)" dir=out action=allow
program=%UPPATH%
```

```
shutdown /r /t 300
```

## **ЦЕНТР ОБРОБКИ ДАНИХ:**

**Товариство з обмеженою  
відповідальністю «ППЛ 33-35»**

**Генеральний**

**директор \_\_\_\_\_ О.О.Федоров**

## **КОРИСТУВАЧ**

Место для ввода текста.

Место для ввода текста.