

Лекція 5

МЕРЕЖЕВІ МОЖЛИВОСТІ ІНТЕРПРЕТАТОРА CMD

Повторення матеріалу Лекції 4.

1. Написати фрагмент командного файлу, який змінює кодування на зазначене користувачем. Якщо користувач ввів неприпустиме значення — командний файл повинен перезапросити значення кодування.

2. Написати фрагмент командного файлу, який буде запитувати у користувача ім'я файлу і видаляти його, якщо він існує. Якщо файл не існує, командний файл повинен запитати ім'я файлу знову.

3. Записати фрагмент командного файлу, який копіює файл, вказаний в якості першого параметра командного рядка число разів, що вказане в якості другого параметра командного рядка. Копії файлу повинні бути пронумеровані і потрапляти в директорію, де міститься вихідний файл.

Інтерпретатор cmd має потужний інструментарій для взаємодії з мережею. Далі ми розглянемо основні команди, доступні користувачеві з командного рядка.

PING — одна з базових і найкорисніших CMD-команд. Вона відображає якість зв'язку, показує, чи може Ваш комп'ютер надсилати дані за цільовою IP-адресою, і якщо може, то з якою затримкою (лістинг 5.1.).

```
D:\>PING google.com
Pinging google.com [172.217.16.46] with 32 bytes of data:
Reply from 172.217.16.46: bytes=32 time=29ms TTL=54
Reply from 172.217.16.46: bytes=32 time=24ms TTL=54
Reply from 172.217.16.46: bytes=32 time=24ms TTL=54
Reply from 172.217.16.46: bytes=32 time=24ms TTL=54
Ping statistics for 172.217.16.46:
```

Лістинг 5.1. — Приклад використання команди PING

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 29ms, Average = 25ms
```

Лістинг 5.1. (закінчення) — Приклад використання команди PING

У команди PING існує ряд корисних ключів (табл. 5.1.), що дозволяють зробити її тонке налаштування.

Таблиця 5.1. — Ключі команди PING

Ключ	Опис
-w <тайм-аут>	Тайм-аут для кожної відповіді (в мілісекундах)
-t	Перевірка зв'язку із зазначеним вузлом до припинення
-n <число>	Число запитів відлуння, що відправляються
-4	Примусове використання протоколу IPv4
-6	Примусове використання протоколу IPv6
-l <розмір>	Розмір буфера відправки
-f	Встановлення в пакеті прапорця, що забороняє фрагментацію (тільки IPv4)

Звичайно, з командою PING також працюють оператори перенаправлення вводу/виводу.

TRACERT означає Trace Route. Як і PING, команда висилає пакет даних для виявлення мережових проблем. Однак, вона визначає не затримку відправки і повернення пакета, а його маршрут (лістинг 5.2.):

```
TRACERT <ім'я_призначення або адреса_IP> [-d] [-h
<максимальна_кількість_переходів>] [-j <список_вузлів>] [-w <таймаут>]
```

```
D:\>TRACERT google.com
```

```
Tracing route to google.com [172.217.16.46]  
over a maximum of 30 hops:
```

```
 1      2 ms      2 ms      1 ms  router.asus.com [192.168.1.1]  
 2      2 ms      2 ms      2 ms  vipa11.te.net.ua [195.138.80.162]  
 3     18 ms     16 ms     18 ms  vgw1-vipas.te.net.ua [195.138.70.177]  
 4      2 ms      2 ms      2 ms  core3-gw-vgw1.te.net.ua [195.138.67.216]  
 5     19 ms      2 ms      2 ms  br3-co-core3-dca.te.net.ua [195.138.67.204]  
 6     14 ms     16 ms     11 ms  google-gw.te.net.ua [195.138.70.134]  
 7     11 ms     11 ms     11 ms  108.170.248.131  
 8     12 ms     11 ms     15 ms  108.170.234.224  
 9     25 ms     25 ms     24 ms  216.239.46.121  
10     26 ms     25 ms     28 ms  108.170.250.209  
11     25 ms     24 ms     25 ms  216.239.41.133  
12     24 ms     24 ms     26 ms  muc03s08-in-f46.1e100.net [172.217.16.46]
```

```
Trace complete.
```

Лістинг 5.2. — Приклад використання команди TRACERT

Команда TRACERT також має ряд ключів для її тонкої настройки (табл. 5.2.).

Таблиця 5.2. — Ключі команди TRACERT

Ключ	Опис
-d	Прискорює виконання команди TRACERT за рахунок відмови від перетворення адрес IP маршрутизаторів в доменні імена
-h <максимальна_кількість_переходів>	Використовується для вказання максимальної кількості переходів на шляху до точки призначення. За замовчуванням використовується значення 30
-j <список_вузлів>	Дозволяє вказати проміжні точки призначення у вигляді списку адрес IP, розділених пробілами (<i>список_вузлів</i>). Цей параметр використовує Loose Source Routing, що дозволяє вставляти один або кілька маршрутизаторів між проміжними пунктами. Цей ключ дозволяє вказати до дев'яти проміжних вузлів
-w <таймаут>	Використовується для вказання часу (в мілісекундах) очікування відповіді ICMP Time Exceeded або відповіді Echo Reply на тестовий запит. За замовчуванням використовується значення 4000 (4 секунди)

Команда PATHPING аналогічна TRACERT, однак, вона більш інформативна, а тому вимагає більше часу для виконання. Вона аналізує маршрут пакетів даних і визначає, на яких проміжних вузлах сталася втрата:

PATHPING <ім'я_призначення або адреса_IP> [-n] [-h
<Максимальна_кількість_переходів>] [-g <список_вузлів>] [-p <період>] [-q
<кількість_запитів>] [-w <timeout>] [-T] [-R]

Основні ключі команди PATHPING наведені у табл. 5.3.

Таблиця 5.3. — Ключі команди PATHPING

Ключ	Опис
-n	Прискорює виконання команди за рахунок відмови від перетворення адрес IP в імена
-h <максимальна_кількість_переходів>	Вказує максимальну кількість маршрутизаторів до точки призначення (за замовчуванням 30)
-g <список_вузлів>	Поміщає в заголовки тестових пакетів ICMP параметр Loose Source Router
-p <період>	Дозволяє вказати час в мілісекундах (ms), який команда чекатиме між послідовними запитам (за замовчуванням 250)
-q <кількість_запитів>	Дозволяє вказати кількість тестових запитів до кожного маршрутизатора в мережі (за замовчуванням 100)
-w <очікування_відповіді>	Дозволяє встановити час (в мілісекундах) очікування відповіді від кожного маршрутизатора (за замовчуванням 3000 мс або 3 с)
-T	Використовується для перевірки наявності Quality of Service (QoS)
-R	Так само використовується для виявлення QoS; визначає підтримку Resource Reservation Protocol (RSVP) кожним пристроєм на маршруті

Наступною найважливішою командою є команда IPCONFIG. Ця команда найбільш часто використовується для налаштування мереж в Windows. І справа не

тільки в обсязі інформації, яку вона надає, але і в тому, що вона комбінується з декількома ключами, що розширюють її можливості (лістинг 5.3.).

```
D:\>IPCONFIG

Windows IP Configuration

Wireless LAN adapter Local Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Wireless LAN adapter Wireless Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::8136:2c54:dee:9617%14
    IPv4 Address. . . . . : 192.168.1.217
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

Лістинг 5.3. — Приклад використання команди IPCONFIG

У табл. 5.4. наведені ключі команди IPCONFIG.

Таблиця 5.4. — Ключі команди IPCONFIG

Ключ	Опис
/all	Відображення повної інформації про всі адаптери
/release [адаптер]	Відправлення повідомлення DHCPRELEASE серверу DHCP для звільнення поточної конфігурації DHCP і видалення конфігурації IP-адрес для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера
/renew	Оновлення IP-адреси для певного адаптера або, якщо адаптер не заданий, то для всіх. Доступно тільки при налаштованому автоматичному отриманні IP-адрес
/flushdns	Очищення DNS кеша
/registerdns	Оновлення всіх зарезервованих адрес DHCP і перереєстрація імен DNS

Закінчення таблиці 5.4.

/displaydns	Відображення вмісту кеша DNS
/showclassid адаптер	Відображення коду класу DHCP для зазначеного адаптера. Доступно тільки при налаштованому автоматичному отриманні IP-адрес
/setclassid адаптер [код_класа]	Зміна коду класу DHCP. Доступно тільки при налаштованому автоматичному отриманні IP-адрес

Ще одна важлива мережева команда — GETMAC. Вона дозволяє дізнатися власну MAC-адресу, яка прописана в самому пристрої (лістинг 5.4.):

GETMAC [/S система [/U користувач [/P пароль]]] [/FO формат] [/NH] [/V]

Так, кожний сумісний зі стандартами IEEE 802 пристрій має унікальну MAC-адресу (Media Access Control), яку виробник присвоює кожній одиниці.

D:\>GETMAC	
Physical Address	Transport Name
=====	
=====	
00-50-56-C0-00-01	\Device\Tcpip_{D4302FD9-C121-494B-A719-8231E8673652}
00-50-56-C0-00-08	\Device\Tcpip_{72E2099B-9799-4B2F-A476-04E5BF30AF11}
F8-28-19-27-58-CA	\Device\Tcpip_{8BC43119-FAD5-498A-A498-C1FFCD4056E3}

Лістинг 5.4. — Приклад використання команди GETMAC

Ключі команди GETMAC наведено у табл. 5.5.

Таблиця 5.5. — Ключі команди GETMAC

Ключ	Опис
/S система	Адреса або ім'я віддаленого комп'ютера, до якого буде виконано підключення
/U домен \користувач	Призначений для користувача контекст, в якому буде виконуватися команда
/P пароль	Пароль для цього користувача контексту. Виконується запит пароля, якщо він не заданий
/FO формат	Формат, в якому слід відображати результати запиту. Допустимі формати: "TABLE", "LIST", "CSV"
/NH	Вказує, що рядок заголовків стовпців не повинен відображатися в результуючому файлі форматів TABLE і CSV
/V	Режим відображення докладної інформації

NSLOOKUP (англ. Name server lookup — пошук на сервері імен) — утиліта, що надає користувачеві інтерфейс командного рядка для звернення до системи DNS (простіше кажучи, DNS-клієнт) (лістинг 5.5.). Програма дозволяє працювати користувачеві в двох режимах: інтерактивному і неінтерактивному. У першому випадку користувач, потрапивши в командний рядок NSLOOKUP, має можливість виконувати команди NSLOOKUP, у другому випадку — звіти отримують шляхом задавання аргументів командного рядка інтерпретатора.

```
D:\>NSLOOKUP wikipedia.org
Server:  router.asus.com
Address:  192.168.1.1
Non-authoritative answer:
Name:     wikipedia.org
Addresses: 2620:0:862:ed1a::1
          91.198.174.192
```

Лістинг 5.5. — Приклад використання команди NSLOOKUP

Всередині команди NSLOOKUP реалізована своя підсистема команд. Коротко розглянемо найважливіші з них:

1. Команда NSLOOKUP LS використовується для відображення вмісту певної зони на сервері DNS:

ls [параметр] <домен>

Параметр <домен> використовується для вказівки зони, вміст якої необхідно переглянути:

-d — повертає всі записи в зазначеному домені;

-h — повертає інформацію про центральний процесор і операційну систему зазначеного домену, якщо в дані зони входить запис HINFO (інформація про вузол);

-s — повертає відомі служби систем в зазначеному домені.

2. Команда NSLOOKUP LSERVER. При запуску утиліти NSLOOKUP в інтерактивному режимі підключення здійснюється до локального сервера перетворення імен або до сервера, зазначеного в якості параметра при запуску команди.

3. Команда NSLOOKUP SERVER. Команда SERVER працює таким же чином, як і команда LSERVER, крім того, що для пошуку адреси нового сервера перетворення імен використовується поточний прийнятий за замовчуванням сервер DNS, на відміну від використання сервера імен, що визначається при роботі NSLOOKUP (лістинг 5.6.).

```
D:\>NSLOOKUP
Default Server:  router.asus.com
Address:  192.168.1.1

> LSERVER 8.8.8.8
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8
```

Лістинг 5.6. — Приклад використання команди NSLOOKUP SERVER

Розглянемо команду NETSTAT. Ця утиліта є засобом для збору статистики, аналізу та діагностики. Якщо дана команда вводиться без параметрів, вона відображає список всіх поточних активних підключень (лістинг 5.7.).

D:\>NETSTAT			
Active Connections			
Proto	Local Address	Foreign Address	State
TCP	192.168.1.217:51549	40.67.251.132:https	ESTABLISHED
TCP	192.168.1.217:51551	40.67.251.132:https	ESTABLISHED
TCP	192.168.1.217:51553	lg-in-f188:https	ESTABLISHED
TCP	192.168.1.217:51701	a2-17-156-15:https	CLOSE_WAIT
TCP	192.168.1.217:51703	93.184.220.29:http	CLOSE_WAIT
TCP	192.168.1.217:51721	52.114.128.8:https	TIME_WAIT
TCP	192.168.1.217:51722	waw02s17-in-f3:https	TIME_WAIT
TCP	192.168.1.217:51723	13.107.3.128:https	ESTABLISHED

Лістинг 5.7. — Приклад використання команди NETSTAT

Основні ключі команди NETSTAT наведені а табл. 5.6.

Таблиця 5.6. — Основні ключі команди NETSTAT

Ключ	Опис
-a	Показує всі з'єднання і порти, що знаходяться в режимі очікування
-e	Відображає статистику Ethernet
-n	Показує адреси та порти в цифровому форматі (адреси IP замість імен інтерфейсів)
-o	Відображає ідентифікатор процесу-власника для кожного з'єднання
-p <протокол>	Показує з'єднання для зазначеного протоколу. Можна вибрати один з таких протоколів: TCP, TCPv6, UDP і UDPv6. При вказівці параметра -s можна вказувати IP, IPv6, ICMP і ICMPv6
-r	Показує таблицю маршрутизації системи

-s	Відображає статистику для кожного протоколу окремо; за замовчуванням статистика відображається для протоколів TCP, TCPv6, UDP і UDPv6, IP, IPv6, ICMP і ICMPv6. Підмножина протоколів може бути зазначеною за допомогою параметра -p
----	--

Однією з найбільш універсальних мережеских утиліт командного рядка є утиліта TELNET.

TELNET — інтерфейс доступу до однойменного мережевого протоколу для реалізації текстового інтерфейсу по мережі (в сучасній формі — за допомогою транспорту TCP).

Використовуючи даний протокол, ми можемо взаємодіяти практично з будь-яким мережеским сервісом. Розглянемо приклад взаємодії з сервером відправки листів — SMTP.

Особливо відзначимо, що за замовчуванням команда TELNET не встановлюється з операційною системою Windows. Проте, виконавши кілька простих кроків ми можемо легко довантажити її.

Для цього достатньо виконати команду довантаження відповідного компонента Windows:

PKGMR /iu: "TelnetClient"

Приклад встановлення команди TELNET показаний у лістингу 5.8.

```
D:\>PKGMR /iu:"TelnetClient"
```

Лістинг 5.8. — Приклад встановлення команди TELNET

Синтаксис команди без додаткових ключів виглядає наступним чином:

TELNET Вузол [Порт]

Підключимося, наприклад, до SMTP сервера smtp.te.net.ua через стандартний порт 25 (лістинг 5.9.).

```
D:\>TELNET smtp.te.net.ua 25
220 te.net.ua ESMTP CommuniGate Pro 6.2.7 is glad to see you!
```

Лістинг 5.9. — Приклад підключення до SMTP сервера за допомогою команди TELNET

Після запрошення сервера нам пропонується вводити будь-які доступні SMTP команди, основні з яких наведені в табл. 5.7.

Таблиця 5.7. — Основні команди протоколу SMTP

Команда	Синтаксис	Опис
HELLO (HELO)	HELO <SP> <domain> <CRLF>	Ця команда використовується щоб ідентифікувати SMTP-відправника на приймаючому сервері. У разі успішного виконання цієї команди одержувач і відправник готові до подальшої роботи
MAIL (MAIL)	MAIL <SP> FROM:<reverse-path> <CRLF>	Ця команда використовується щоб відправити пошту одному або більше адресатам. Параметром команди є Ваша e-mail адреса. (MAIL FROM: mypost@mail.net)
RECIPIENT (RCPT)	RCPT <SP> TO:<forward-path> <CRLF>	Ця команда використовується щоб визначити одного одержувача пошти. Множина одержувачів визначаються множиною цих команд. (RCPT TO yourpost@mail.net)
DATA (DATA)	DATA <CRLF>	За допомогою цієї команди серверу передається текст повідомлення
SEND (SEND)	SEND <SP> FROM:<reverse-path> <CRLF>	Ця команда використовується для можливості відправки поштових даних на один або більше поштових терміналів. Аргумент команди містить в собі зворотний маршрут. Команда вважається успішно виконаною, якщо повідомлення буде успішно доставлено на термінал
QUIT (QUIT)	QUIT <CRLF>	Ця команда визначає, що одержувач повинен надіслати команду OK і потім закрити канал передачі

З огляду на команди, наведені в табл. 5.7. проведемо автентифікацію на нашому SMTP сервері (лістинг 5.10.).

```
AUTH LOGIN
334 VXNlcm5hbWU6
YWxhcnQ=
334 UGFzc3dvcmQ6
*****=
235 alart@te.net.ua relaying authenticated
```

Лістинг 5.10. — Автентифікація на SMTP сервері

Відзначимо, що логін і пароль вводиться в форматі Base64.

Base64 — стандарт кодування двійкових даних за допомогою тільки 64 символів ASCII. Алфавіт кодування містить текстово-цифрові латинські символи A,...,Z, a,...,z і 0,...,9 (62 знака) і 2 додаткових символи, що залежать від системи реалізації. Кожні 3 вихідних байти кодуються 4 символами (збільшення розміру на $\frac{1}{3}$).

Ця система широко використовується в електронній пошті для подання бінарних файлів в тексті листа (транспортне кодування).

За допомогою команди MAIL вкажемо відправника нашого повідомлення, за допомогою команди RCPT вкажемо одержувача повідомлення, за допомогою команди DATA вкажемо текст нашого повідомлення (лістинг 5.11.).

```
MAIL FROM: alart@te.net.ua
250 alart@te.net.ua sender accepted
RCPT TO: radiosquid@gmail.com
250 radiosquid@gmail.com will relay mail for an authenticated user
DATA
354 Enter mail, end with "." on a line by itself
To: radiosqui@gmail.com
From: alart@te.net.ua
Subject: Test
Hello! This is test.
.
250 721978012 message accepted for delivery
QUIT
221 te.net.ua CommuniGate Pro SMTP closing connection
Connection to host lost.
```

Лістинг 5.11. — Приклад відправлення повідомлення

Аналогічним чином ми можемо використовувати TELNET і для підключення до POP3 серверів.

Основні команди для роботи з POP3 наведені в табл. 5.8.

Таблиця 5.8. — Основні команди POP3

Команда	Опис команди
USER username	Перша команда, яка дається після підключення до сервера. Вона повинна складатися тільки з імені користувача обов'язково без доменного суфікса
PASS userpassword	Наступна команда після USER. Вона містить пароль користувача
STAT	Відповідь цієї команди покаже нам, скільки у нас листів і який обсяг в байтах вони займають
LIST	Виводить список повідомлень і їх розмір в байтах
RETR numbermsg	Відображає у вікні TELNET лист під номером numbermsg
TOP numbermsg lines	Додаткова команда, її підтримують не всі POP3 сервера, вона відобразить заголовок повідомлення і перші його рядки. Наприклад, TOP 1 0 виведе тільки заголовок повідомлення 1, а TOP 1 5 виведе заголовок і перші 5 рядків тексту повідомлення
DELE numbermsg	Ставить мітку на видалення повідомлення під номером numbermsg і видалить їх після команди QUIT. Якщо команда QUIT не дана, а з'єднання було перервано, то повідомлення не будуть видалені
RSET	Знімає мітки на видалення повідомлень, що раніше були поставлені командою DELE.
QUIT	Після введення цієї команди сервер видалить всі помічені повідомлення і відключить Вас від поштової скриньки

Наведемо приклад роботи з POP3 сервером. Підключимося до нього через стандартний порт 110, пройдемо автентифікацію, запитаємо список листів, які є на сервері, виведемо на екран вміст кількох повідомлень (лістинг 5.12.).


```

D:\>TELNET pop3.te.net.ua 110
+OK te.net.ua CommuniGate Pro POP3 Server 6.2.7 ready
USER alart
+OK please send the PASS
PASS mamapapa
+OK 5 messages (11915 bytes)
LIST
+OK 5 messages
1 1547
2 1159
3 3093
4 1528
5 4588
.
RETR 1
+OK 1547 bytes will follow
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed; d=te.net.ua; h=date:from
:message-id:to:mime-version:content-type
:content-transfer-encoding; s=relay1; bh=nXI52SzMXcK6FURs/JhRKZo
SVxc=; b=nUBhmYIPVCAT/ygMyBlPl1eK8dLmCOUJexhp5GS63PHUuHCdksL92GU
oFcrGo2ySxgavjlxZhZNRytqWjQGrF+0UoylC1qv+Iq6wp4gR0QSkia0ojKdTTtM
zoRhidxc2fV4fL2E1/+AHdLTMIC31mY107XGN2FYNuMLk4g4YjB8=
X-Spam-Flag: NO
X-Spam-Score: score=-127.8 required=5.0 tests=ALL_TRUSTED,BAYES_50,
MISSING_SUBJECT,USER_IN_WHITELIST autolearn=disabled version=3.2.5
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on te.net.ua
RETR 2
+OK 1159 bytes will follow
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed; d=te.net.ua; h=date:from
:message-id:to:subject:mime-version:content-type
:content-transfer-encoding; s=relay1; bh=/edzoYuyn17WXm8KeqcX/R+
khdQ=; b=AJyjmkbOGddxpkHlknBgBZZz1xJRN3Ru98k+OILK7UKpA9/g9h3HLoD
265oZ6dA1XSzhVYbnqm0dwiFX+g3lflPg3zYLcETIjCI2kvoTT7nSYyr4g75yfOY
Jl3LQDAvJyXqV8GU8TX42BqrcXsjDhFZKJB3NpGPUPr5bYUrrn1k=
X-Spam-Flag: NO
X-Spam-Score: score=-125.6 required=5.0 tests=ALL_TRUSTED,BAYES_50,
TVD_SPACE_RATIO,USER_IN_WHITELIST autolearn=disabled version=3.2.5
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on te.net.ua

```

Лістинг 5.12. — Приклад роботи з POP3 сервером

Відзначимо при цьому, що прямо неможливо управляти командою TELNET через командний файл. Доступ до управління командою TELNET може бути отриманий за допомогою мови VBScript.

Відзначимо, що деякі дії в операційній системі повинні виконуватися з певною періодичністю. Розглянемо далі питання планування завдань.

Для планування завдань використовується команда `SCHTASKS`, яка дозволяє адміністратору створювати, видаляти, змінювати і опитувати заплановані завдання в локальній або віддаленій системі:

SCHTASKS / параметр [аргументи]

/Create — створення запланованого завдання;

/Delete — видалення запланованого завдання або завдань;

/Query — виведення даних про всі заплановані завдання;

/Change — зміна властивостей запланованого завдання;

/Run — виконання запланованого завдання на вимогу.

Наведемо приклад отримання інформації про існуючі заплановані завдання (лістинг 5.13.).

D:\>SCHTASKS /Query			
Folder: \			
TaskName	Next Run Time	Status	
=====	=====	=====	
=====			
ATK Package A22126881260	N/A	Ready	
NvProfileUpdaterDaily_{B2FE1952-0186-46C	6/15/2019 12:25:10 PM	Ready	
NvProfileUpdaterOnLogon_{B2FE1952-0186-4	N/A	Ready	
NvTmMon_{B2FE1952-0186-46C3-BAEC-A80AA35	N/A	Ready	
NvTmRepOnLogon_{B2FE1952-0186-46C3-BAEC-	N/A	Ready	
NvTmRep_{B2FE1952-0186-46C3-BAEC-A80AA35	6/15/2019 12:25:10 PM	Ready	
OneDrive Standalone Update Task-S-1-5-21	6/15/2019 2:15:13 PM	Ready	
Opera scheduled Autoupdate 1518965635	6/16/2019 9:51:23 AM	Ready	

Лістинг 5.13. — Приклад отримання інформації про існуючі

заплановані завдання

Для того, щоб створити нову задачу за розкладом використовується наступна команда:

```

SCHTASKS /Create [/S <система> [/U <користувач> [/P [<пароль>]]]]
[/RU <ім'я_користувача> [/RP <пароль>]] /SC <розклад>
[/MO <модифікатор>] [/D <день>]
[/M <місяць>] [/I <простоювання>] /TN <ім'я_завдання> /TR <виконання>
[/ST <час_початку>]
[/RI <інтервал>] [ {/ET <час_закінчення> | /DU <тривалість>}
[/K]
[/XML xmlfile] [/V1]]
[/SD <дата_запуску>] [/ED <дата_закінчення>] [/IT | /NP] [/Z] [/F]

```

Розглянемо кілька основних ключів, які наведені у табл. 5.9.

Таблиця 5.9. — Основні ключі команди SCHTASKS

Ключ	Опис
/SC розклад	Задає частоту повторення завдання. Можливі наступні типи розкладу: MINUTE, HOURLY, DAILY, WEEKLY, MONTHLY, ONCE, ONSTART, ONLOGON, ONIDLE, ONEVENT
/МО <модифікатор>	Уточнення типу розкладу для більш детального контролю за періодичністю
/D <день>	День тижня, на який заплановано виконання завдання. Можна вибрати зі значень MON, TUE, WED, THU, FRI, SAT, SUN і для розкладів типу MONTHLY — з 1 по 31 (дні місяця). Підстановлювальний знак «*» вказує всі дні
/K	Завершення завдання по досягненні часу завершення або при перевищенні тривалості. Цей параметр непридатний для наступних типів розкладу: ONSTART, ONLOGON, ONIDLE, ONEVENT. Цей параметр повинен використовуватися разом з /ET або /DU
/TN <ім'я задачі>	Ім'я, що однозначно ідентифікує заплановане завдання
/TR <програма>	Шлях і ім'я файлу програми, яка повинна бути запущена в призначений час. Приклад: C:\Windows\System32\calc.exe

Закінчення таблиці 5.9.

/ST <час_початку>	Час запуску завдання. Формат вказання часу: ГГ:ХХ (24-годинний), наприклад, 14:30 замість 2:30 PM. Якщо параметр /ST не заданий, то за замовчуванням використовується поточний час. Цей параметр повинен використовуватися разом з /SC ONCE
/ET <час_завершення>	Час завершення виконання завдання. Формат вказання часу: ГГ:ХХ (24-годинний), наприклад, 14:50 замість 2:50 PM. Цей параметр непридатний для наступних типів розкладу: ONSTART, ONLOGON, ONIDLE, ONEVENT

Наведемо приклад запуску гри FREECELL в першу неділю кожного місяця:

```
SCHTASKS /Create /SC MONTHLY /MO first /D SUN /TN гра  
/TR c:\freecell\cell.exe
```

Створення призначеного завдання «гра» для запуску freecell.exe починаючи з 12:00 з автоматичним завершенням о 14:00 щодня:

```
SCHTASKS /Create /SC DAILY /TN гра /TR c:\freecell\cell.exe /ST 12:00  
/ET 14:00 /K
```

Домашнє завдання до Лекції №5.

Записати фрагмент коду, який відправляє лист по протоколу SMTP. Перевірити код на конкретному сервері.