УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК» Коледж економіки, права та інформаційних технологій

Циклова комісія з інформаційних технологій

добришини ю.**с., чернозубкін і.о.**

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ ЗАНЯТЬ З ДИСЦИПЛІНИ «АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ»

(для студентів спеціальностей 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки»

Київ – 2019 р.

УДК 004.416

Розглянуто на засіданні циклової комісії з інформаційних технологій протокол № 1 від «28» серпня 2019 р. Рекомендовано до видання методичною радою Коледжу економіки, права та інформаційних технологій Університет економіки та права «КРОК» протокол № 1 від «30» серпня 2019 р

Автори: Ю.Є. Добришин, кандидат технічних наук, доцент кафедри комп'ютерних наук Навчально-наукового інституту інформаційних та комунікаційних технологій «Університет економіки та права «КРОК»

I.O. Чернозубкін, кандидат технічних наук, доцент кафедри комп'ютерних наук Навчально-наукового інституту інформаційних та комунікаційних технологій «Університет економіки та права «КРОК»

[Текст]: Методичні рекомендації для виконання лабораторних робіт з дисципліни АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ / [Ю. Є. Добришин, І.О.Чернозубкін]; Університет економіки та права «КРОК» – Київ - 2019. – 49 с.

Методичні рекомендації для виконання лабораторних робіт містять теоретичні та практичні питання з найбільш важливих тем навчальної дисципліни «Адміністрування програмних систем і комплексів» та визначають порядок та технологію виконання технологічних операцій з адміністрування сучасних інформаційно-телекомунікаційних систем.

Видання призначене для студентів спеціальностей 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» денної форми навчання.

РОЗГЛЯНУТО І СХВАЛЕНО

Педагогічною радою Коледжу економіки, права та інформаційних технологій Протокол № 1 від «30» серпня 2019 р.

УДК 004.416 ©Добришин Ю.Є. 2019 р. ©Чернозубкін І.О. 2019 р. © Коледж економіки, права та інформаційних технологій ©Університет економіки та права «КРОК» 2019 р.

ВСТУП 4
КРИТЕРІЇ ОЦІНКИ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ 5
Лабораторна робота №1 Основні програмні інструменти щодо адміністрування
Windows
Лабораторна робота №2 Перевірка стану служб операційного середовища
Windows
Лабораторна робота №3 Моніторинг операційної системи за допомогою
програмного забезпечення Performance Monitor
Лабораторна робота №4 Перегляд журналів подій та системного журналу
безпеки операційної системи Windows
Лабораторна робота №5 Перевірка функціонування та величини завантаження
локальної мережі, швидкості та активності роботи контролеру домену 47
Лабораторна робота №6 Робота з доменними груповими політиками в
середовищі MS Windows Server
Лабораторна робота №7 Налаштування брандмауера ОС Windows 64
Лабораторна робота №8 Встановлення та налаштування VPN з'єднання MS
Windows Server
МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАНЯТТЬ 85
РЕКОМЕНДОВАНА ЛІТЕРАТУРА 85

ВСТУП

Метою навчальної дисципліни «Адміністрування програмних систем та комплексів» є формування у слухачів рівня інформаційної культури, отримання знань та практичних навиків з виконання операцій з адміністрування програмних систем та комплексів, оволодіння методиками та правилами планування заходів щодо здійснення основних операції з адміністрування операційних систем та баз даних, програмних додатків та мережевих компонентів, розташованих на базі серверного обладнання та персональних комп'ютерів.

Програма дисципліни передбачає проведення лабораторних занять завданнями, яких є формування практичних навичок у відповідності з поставленою метою.

За результатами відпрацювання лабораторних робіт студенти повинні вміти:

1. Виконувати операції зі встановлення, налаштування та адміністрування системного та загальносистемного програмного забезпечення сучасних операційних систем (далі-OC) Windows.

2. Проводити моніторинг продуктивності роботи та підтримувати працездатність програмних систем і комплексів в процесі їх супроводження.

3. Здійснювати роботи з перевірки стану служб операційного середовища, журналів подій та системного журналу безпеки операційної системи Windows

4. Встановлювати, налагоджувати програмне забезпечення брандмауера OC Windows.

5. Налаштовувати роботу користувачів з доменними груповими політиками в середовищі MS Windows Server

6. Здійснювати операції зі встановлення та налаштування VPN з'єднання на базі операційної системи Windows .

ОЦІНКИ ЗА ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Основа мета перевірки виконання лабораторних робіть – виявлення здатності студента застосовувати одержані теоретичні знання на практиці.

Оцінка за виконання лабораторного заняття ставиться як середньоарифметична суми оцінок безпосередньо за виконану роботу та захист.

Оцінка "відмінно" ставиться, якщо результати виконання роботи збігаються з результатами контрольного прикладу, завдання до лабораторної роботи виконані в повному обсязі, студент демонструє знання про матеріали роботи на рівні 90–100 %.

Оцінка "добре" – якщо результати виконання роботи частково збігаються з результатами контрольного прикладу, завдання до лабораторної роботи виконані в повному обсязі, але студент демонструє знання матеріалів роботи на рівні 75–90 %.

Оцінка "задовільно" – якщо результати виконання роботи частково збігаються з результатами контрольного прикладу, завдання до лабораторной роботи виконані не в повному обсязі, студент демонструє знання наведеного матеріалу роботи на рівні 50–75 %.

Оцінка "незадовільно" – якщо студент не виконав завдання, що зазначені у лабораторної роботі, не відповідає на теоретичні питання, які відносяться до теми роботи.

Лабораторна робота №1

Основні програмні інструменти щодо адміністрування Windows

Метою роботи є вивчення та відпрацювання слухачами програмних засобів щодо адміністрування програмного забезпечення операційної системи Windows (далі – ОС), порядку встановлення та налаштування віддаленого програмного забезпечення з адміністрування компонентів Windows.

Технічне забезпечення занять

1. Персональне робоче місце студента (ПЕОМ) зі встановленим загальносистемним програмним забезпеченням (ОС Windows)

2. Програмне забезпечення віртуалізації OracleVBox.

3. Спеціалізоване програмне забезпечення MS Office, версії ОС Windows.

Питання, що відпрацьовуються на занятті

1. Встановлення програмного забезпечення OracleVBox та його налаштування.

2. Призначення та перевірка роботи програмних компонентів щодо адміністрування операційної системи Windows.

3. Встановлення та налаштування програмного забезпечення щодо віддаленого адміністрування операційної системи Windows.

Приклад виконання завдань:

1. Вхід в меню управління комп'ютером

1.1 Для запуску основних інструментів адміністрування слід відкрити вкладку управління. Це можна зробити двома способами:

1.2. Увійти в меню «Пуск» і, натиснувши правою кнопкою на пункті «Комп'ютер», вибрати «Управління» або натиснувши на клавіші Win» і «R», відкривши вікно виконання команд і ввівши «compmgmtlauncher».

1.3 Після цього відкривається вікно управління системою, де представлені всі основні інструменти, які дозволять повністю налаштувати її для своїх потреб.

1.4. Ці ж програми і служби можна запускати і окремо (для чого існують спеціальні команди) або через пункт «Адміністрування».

Файл Действие Вид Справ	(3	
Управление компьютером (л	Имя	Действия
Служебные программы	🖞 Служебные программы	Управление компьютеро
 С Планировщик задании Просмотр событий Общие папки Локальные пользовате Производительность Диспетчер устройств Диспетчер устройст Запоминающие устройст Управление дисками Службы и приложения 	Запоминающие устройства Службы и приложения	Дополнительные дей

Рис 1 Виклик вікна «Управление компьютером»

2. Редактор ресстру

2.1. Використовувати засоби для редагування реєстру часто доводиться при виникненні яких-небудь проблем з шкідливими кодами або програмами автозавантаження. Також він буде корисний при видаленні слідів яких-небудь додатків (у тому числі і вірусів, хоча не обов'язково). Запустити редактор можна, відкривши вікно виконання (Win+R) і ввівши команду «**regedit**».

2.2. При його редагуванні слід пам'ятати, що варто змінювати тільки ті пункти, призначення яких користувач впевнений. Інакше можна порушити роботу комп'ютера і навіть призвести до необхідності переустановлення програм, драйверів або всієї операційної системи. (рис 2).

📸 Редактор реестра				
Файл Правка Вид Избранное Справка				10 ¹ 210
⊳-J SeCEdit ▲	Имя	Тип	Значение	
b - ja setup	💩 (По умолчанию)	REG_SZ	mnmsrvc	
SoftwareProtectionPlatform	ab AppInit_DLLs	REG_SZ		
Superfetch	100 DdeSendTimeout	REG_DWORD	0x00000000 (0)	
superierch	🕫 DesktopHeapLo	REG_DWORD	0x00000001 (1)	
SystemRestore	(ab) DeviceNotSelect	REG_SZ	15	
Terminal Server	👪 GDIProcessHan	REG_DWORD	0x00002710 (10000)	
Time Zones	ab IconServiceLib	REG_SZ	IconCodecService.dll	
🤞 🛺 Tracing	🐯 LoadAppInit_DLLs	REG_DWORD	0x00000000 (0)	
b 📗 UnattendSettings	🐯 Shutdown Warni	REG_DWORD	0xffffffff (4294967295)	
	ab) Spooler	REG_SZ	yes	
	(ab) TransmissionRet	REG_SZ	90	
	USERNestedWin	REG_DWORD	0x0000032 (50)	
Winlogon	USERPostMessa	REG_DWORD	0x00002710 (10000)	
b- Winsat	🐯 USERProcessHa	REG_DWORD	0x00002710 (10000)	
WinSATAPI				
Windows Photo Viewer				
Windows Portable Devices				
Windows Script Host				
Windows Search				
Wisp				
>> Workspaces				
🔊 🌗 WwanSvc				
👂 - 📕 Mozilla				
NVIDIA Corporation				
p				
Policies				
RegisteredApplications				
Sonic				
Wax6422Node				
SVSTEM				
HKEY USERS				
HKEY CURRENT CONFIG				

Рис 2 Вид «Редактору реєстру» ОС Windows

3. Редактор локальних користувачів і груп

3.1. Можливість редагування як окремих користувачів ПК, так і їх груп надана не для всіх версій Windows – тільки для професійних (рис. 3).

3.2. Зате з її допомогою можна налаштувати і систему, і можливості доступу до неї різних людей, дозволяючи їм користуватися одними програмами, і забороняючи запускати інші.



Рис.3 Робота з обліковими записами користувачів і груп

4. Служби

4.1. Вкладка служб відкриває доступ до списку. Тут представлені всі наявні в операційній системі служби, включаючи запущені або відключені (рис.4)

4.2. Частина з них працює автоматично і без особливої необхідності в роботу цих процесів втручатися не варто.

4.3. Однак є служби, якими керують вручну – це може бути, наприклад, програма або утиліта оновлення.

*** 📶 🛄 🖳 😬 🔛 🛄 💌							
Управление компьютером (локальным)	🕘 Службы						Действия
Панировшик заланий			0	0.0000000000000000000000000000000000000	T	D A	Службы
В Просмотр событий	Adobe Acrobat Update Service	ИМЯ	Описание	Состояние	і ип запуска	BXC	Допо
» 🙀 Общие папки	Запустить службу	360 Total Security	PROVIDENT OF THE REAL	Работает	Автоматиче	Jloi	Adaba Ass
🖌 🌉 Локальные пользователи и группы		Adobe Acrobat U	Adobe Acr		Вручную	JIOI E	Adobe Acr
📔 Пользователи	25	BranchCache	Эта служб	2.2	Вручную	Cer	Допо.
🚞 Группы	Описание: Adobe Acrobat Undater keeps your	DHCP-клиент	Регистрир	Работает	Автоматиче	/loi	
🔺 🔕 Производительность	Adobe software up to date.	See DNS-клиент	Служба D	Работает	Автоматиче	Cer	
🕨 Средства наблюдения		🥁 KtmRm для коор	Координи		Вручную	Cei	
🖻 📑 Группы сборщиков данных		MBAMService	Malwareby		Автоматиче	Лог	
👂 📑 Отчеты		Microsoft .NET Fr	Microsoft		Отключена	Лог	
🚔 Диспетчер устройств		Microsoft .NET Fr	Microsoft		Отключена	Лоі	
🚰 Запоминающие устройства		Microsoft .NET Fr	Microsoft		Автоматиче	Лог	
😸 Управление дисками		Microsoft .NET Fr	Microsoft		Автоматиче	Лоі	
Службы и приложения		NVIDIA Display Dri	Provides sy		Отключена	Лог	
💁 Службы		Generation Source Eng	Сохранен		Вручную	Лог	
🇃 Управляющий элемент WMI		Parental Controls	Эта служб	Работает	Вручную	Лог	
		🔍 Plug-and-Play	Позволяет		Автоматиче	Лог	
		🍓 Quality Windows	Quality Wi		Вручную	Лоі	
		🔍 Skype Updater	Enables th		Вручную	Лоі	
		🔍 Superfetch	Поддержи	Работает	Автоматиче	Лог	
		🛸 VIA Karaoke digita		Работает	Автоматиче	Лоі	
		🎎 Windows Audio	Управлен	Работает	Автоматиче	Лог	
		🖏 Windows CardSpa	Это обесп		Вручную	Лог	
		🐫 Windows Driver F	Управлен	Работает	Автоматиче	Лог	
		Windows Search	Индексир	Работает	Автоматиче	Лог	
		WMI Performance	Provides p		Вручную	Лог	
		Автонастройка W	Эта служб		Вручную	Ло	
		💁 Автономные фай	Служба ав	Работает	Автоматиче	Лог	
		🗟 Агент зашиты сет	Агент слу		Вручную	Cei	
		а Агент политики I	Безопасно		Вручную	Cer	
					0,000	*	

Рис.4 Служби операційної системи

5. Управління дисками комп'ютера

5.1. Крувати дисками комп'ютера може знадобитися не тільки досвідченому користувачеві. Іноді деякі з дисків (особливо при використанні на комп'ютері декількох вінчестерів або застарілих файлових систем типу FAT32) після переустановки системи стають невидимими. (рис 5).

5.2. І для їх пошуку доведеться зайти в меню «Управления».

:) пасной диск (Е:) резервировано системой	Расположение Простой Простой	Тип Основной	Файловая система NTFS	Состояние	Действия
но и видео (с.)	Простой Простой	Основной Основной Основной	NTFS NTFS NTFS	Исправен (Загрузка, Файл подкач Исправен (Основной раздел) Исправен (Система, Активен, Осн Исправен (Логический диск)	Управлен Допо
циск О овной Зарезерн 18 ГБ 100 МБ N ги Исправен	11 Запасной диск 14,55 ГБ NTFS Исправен (Основ	(С 43,і зной į Исі	;) 96 ГБ NTFS правен (Загрузка, Фай	• Фото и видео (D:) 174,27 ГБ NTFS Исправен (Логический диск)	
D-ROM 0 (F:) носителя					
	иск 0 Зарезері 100 МБ N Исправен D-ROM 0 (F:) носителя	т мск 0 звной 8 ГБ 100 МБ N Исправен 14,55 ГБ NTFS Исправен (Основ 0-ROM 0 (F:) чосителя	т лиск 0 Зарезері Запасной диск (Е:) 14,55 ГБ NTFS Исправен (Основной ј Исправен (Основной ј Исправен (Основной ј Исправен (Основной ј Исправен (Основной ј Исправен (Основной ј	мск 0 Зарезері Запасной диск (Е:) 14,55 ГБ NTFS Исправен (Основной ; 0-ROM 0 (F:) носителя	Миск 0 Зарезері Запасной диск (E:) (С.) Фото и видео (D:) 100 МБ N 14,55 ГБ NTFS 43,96 ГБ NTFS 174,27 ГБ NTFS Исправен Исправен (Основной) Исправен (Загрузка, Фай Исправен (Логический диск) D-ROM 0 (F:) носителя

Рис 5. Меню управління дисками

5.3. За допомогою утиліти управління дисками можна включати і відключати різні розділи на які підключені до ПК вінчестерах, змінювати їх назви та букви. А ще можна вирішити тут проблему з відкриваються флешкою, не користуючись сторонніми програмами.

6. Диспетчер пристроїв

6.1. Для встановлення нового обладнання та вирішення питань з драйверами не обійтися без використання диспетчера пристроїв, вбудованого в систему.



Рис 6. Диспетчер пристроїв

6.2. Крім того, працюючи зі списком пристроїв, їх можна включати і відключати. А також дізнаватися інформацію про кожному, що може знадобитися, наприклад, для перевірки відповідності конфігурації комп'ютера вимогам програми.

7. Диспетчер завдань

7.1. В першу чергу, він виявляється корисним при пошуку шкідливих програм (вірусів), запускають сторонні процеси для виконання комп'ютером.

7.2. За допомогою диспетчеру завдань Windows відбувається настроювання додатків, що завантажуються автоматично разом з системою («Запуск»).

Приложения Процессы Служ	кбы Быстро,	цействи	е Сеть Г	Тользователи	
Имя образа	Пользо	цп	Память (Описание	
360webshield.exe *32	Юрец	00	2 328 KE	360 Internet Security Internet Protection	
chrome.exe *32	Юрец	00	3 188 KE	Google Chrome	
chrome.exe *32	Юрец	00	3 176 KE	Google Chrome	
chrome.exe *32	Юрец	00	14 888 KD	Google Chrome	
chrome.exe *32	Юрец	00	59 288 KB	Google Chrome	
chrome.exe *32	Юрец	00	600 KB	Google Chrome	
chrome.exe *32	Юрец	00	116 096 KB	Google Chrome	
chrome.exe *32	Юрец	00	25 088 KB	Google Chrome	
chrome.exe *32	Юрец	00	76 836 KB	Google Chrome	
cmd.exe *32	Юрец	00	152 KB	Обработчик команд Windows	
conhost.exe	Юрец	00	256 KB	Окно консоли узла	
csrss.exe		00	1 452 KB		
dwm.exe	Юрец	00	8 696 KE	Диспетчер окон рабочего стола	
explorer.exe	Юрец	03	21 536 KB	Проводник	
mmc.exe	Юрец	00	3 576 KB	Консоль управления (ММС)	
mspaint.exe	Юрец	00	19 040 KB	Paint	
OIS.EXE *32	Юрец	00	11 952 KB	Microsoft Office Picture Manager	
QHSafeTray.exe *32	Юрец	00	1 296 KB	360 Total Security	
splwow64.exe	Юрец	00	244 KB	Print driver host for 32bit applications	
taskhost.exe	Юрец	00	956 KB	Хост-процесс для задач Windows	
taskmgr.exe	Юрец	05	2 432 KB	Диспетчер задач Windows	
Viber.exe *32	Юрец	00	107 096 KB	Viber	
•		III)
🛞 Отображать процессы в	сех пользоват	елей		Заверши	ить процесс
🛞 Отображать процессы в	сех пользоват	гелей		Заверши	ить процесс

Рис.7. Диспетчер завдань

8. Журнал подій

8.1. За допомогою цього інструменту можна легко визначити причину неполадок. Щоправда, для його використання необхідні спеціальні знання,

правление компьютером (локальным)	Уровень	Дата и время	Источник	Код события	Категория зад	Действия
Планировшик заланий	🚺 🕕 Сведения	13.04.2016 5:42:35	Security-SPP	903	Отсутствует	Приложе.
🛃 Просмотр событий	Сведения	13.04.2016 5:39:54	LoadPerf	1000	Отсутствует	👩 Откр.
Настраиваемые представления	🕕 Сведения	13.04.2016 5:39:54	LoadPerf	1001	Отсутствует	💚 Созда
👍 🔂 Журналы Windows	Сведения	13.04.2016 5:37:34	Security-SPP	902	Отсутствует	a. 555557555
Приложение	Сведения	13.04.2016 5:37:34	Security-SPP	1003	Отсутствует	
Безопасность	Сведения	13.04.2016 5:37:34	Security-SPP	1066	Отсутствует	Очис
Установка	Сведения	13.04.2016 5:37:32	SecurityCente	r 1	Отсутствует	💎 Филь.
Система	• Сведения	13.04.2016 5:37:30	Security-SPP	900	Отсутствует	Cani
🔲 Перенаправленные события	Сведения	13.04.2016 5:35:39	Search	1003	Служба поиска	CBOM.
🕞 🛗 Журналы приложений и служб	Сведения	13.04.2016 5:35:39	WMI	5617	Отсутствует	Найт.
Подписки	Сведения	13.04.2016 5:35:38	ESENT	302	Ведение журн	Coxp.
🕺 Общие папки	() Сведения	13.04.2016 5:35:36	ESENT	301	Ведение журн	Поне
🌆 Локальные пользователи и группы	Сведения	13.04.2016 5:35:36	ESENT	301	Ведение журн	
Пользователи	Сведения	13.04.2016 5:35:36	ESENT	301	Ведение журн	Вид
📔 Группы	() Сведения	13.04.2016 5:35:34	ESENT	301	Ведение журн	О Обно
Производительность	Сведения	13.04.2016 5:35:34	ESENT	300	Ведение журн	Cona
Средства наблюдения	Сведения	13.04.2016 5:35:34	ESENT	102	Общие	- cnpoi
Группы сборщиков данных	Сведения	13.04.2016 5:35:28	WMI	5615	OTCVTCTBVET	Событие.
р Стчеты	La commente	13.04.3016 5.35.10	Montenan	6000		Свой.
Диспетчер устройств	Событие 903, Securit	y-SPP			×	
запоминающие устроиства						прив
За Управление дисками	Общие Подробн	ости				Ба Копи.
Служов и приложения					<u> </u>	Coxpa
Элравляющий элемент WMI	Служба защиты	программного обеспечен	ия остановлена.		÷	0 Обно
	Имя журнала:	Приложение				🛛 🔽 Спра.
	Источник	Security-SPP	Дата:	13.04.2016 5:42:35		
	Koncoffering	903	Kareropus tastaur	Orogernier		
	Rod coopinia:		согория задачи:	Sicy icity el		
	Уровень:	Сведения	Ключевые слова:	Классический	1	
	Пользов.:	Н/Д	Компьютер:	Юрец-ПК		



9. Планувальник завдань

9.1. У Windows передбачено системне планування виконання ряду завдань. Завдяки цій утиліті можна призначити, наприклад, періодичну дефрагментацію або перевірку диска. Хоча їй же користуються і деякі шкідливі програми.



Рис.9. Вид планувальника завдань

10. Системний монітор

10.1. Користуючись утилітою «системний монітор», можна отримати дані завантаженості деяких складових ПК – пам'яті, процесора і файлу підкачки.



Рис.10. Вид системного монітору

11. Монітор ресурсів

11.1. Частина даних про роботу Windows доступна прямо з диспетчера задач. Однак «монітор ресурсів» забезпечує більш повну картину про використання ресурсів ПК усіма процесами системи. Для цього натисніть кнопку «Пуск».

11.2. У полі пошуку введіть «Монітор ресурсів», а потім у списку результатів виберіть пункт «Монітор ресурсів».



Рис.12. Моніторинг ресурсів

12. Брандмауер

12.1. Завданнями стандартного брандмауера є забезпечення мережевої безпеки. Якщо ж використовувати додаткові налаштування утиліти, можна значно зменшити ймовірність злому вашого ПК і попадання на нього вірусів.

12.2. Використання брандмауера також може заважати і запуску інших, потрібних програм, які доводиться додавати в список виключень.



Рис 12. Вигляд стандартного брандмауера

13. Засоби віддаленого адміністрування

13.1. Адміністрування комп'ютера може здійснювати безпосередньо сам користувач, однак у деяких випадках виникає необхідність забезпечити дистанційне керування. Для надання доступу до одному ПК з іншого потрібна установка і настройка спеціальної програми. Для цього користуються додатком «TeamViewer».

ree license (non-commercial use only) - User	
Allow Remote Control	Control Remote Computer
Please tell your partner the following ID and password if you would like to allow remote control.	Please enter your partner's ID in order to control the remote computer.
Your ID	Partner ID
Password 4687	×
1007	Remote control
Enter a personal password to access this computer	U File transfer
from anywhere.	Connect to partner

Рис.13. Програмне забезпечення «TeamViewer»

Завдання на виконання лабораторної роботи

1. Перевірити встановлення програмного забезпечення **OracleVBox** на робочому місці студента та здійснити в разі необхідності його налаштування.

2. Встановити на віртуальну машину одну з версій операційної системи (Windows 10, Windows 7, Windows XP). Версію ОС студенту призначає викладач.

3. Здійснити перевірку переліку та стану працездатності служб ОС Windows віртуальної машини.

4. Виконати запуск програмного забезпечення «Диспетчер задач Windows» та перевірити його працездатність.

5. За допомогою програмного забезпечення «Диспечера устройств» ОС Windows перевірити працездатність роботи пристроїв операційної системи.

6. Перевірити «Журнал подій» операційної системи Windows віртуальної машини. Переглянути кожний з журналів системи, ознайомитися з інформацією, що надається.

7. Перевірити працездатність програмного забезпечення «Системний моніторинг» та «Моніторинг ресурсів» операційної системи Windows.

8. Запустити програмне забезпечення стандартного брандмауера операційної системи Windows, переглянути роботу його компонентів.

9. Встановити програмне забезпечення «**TeamViewer**» та перевірити його роботу.

10. За результатами робіт підготувати звіт

ЗРАЗОК ЗВІТУ

N⁰	Назва програмного	Стан працездатності	Примітка
3.П.	забезпечення	програмного	
		забезпечення	

Контрольні питання (відповісти письмово)

1. Призначення, характеристика програмного забезпечення OracleVBox.

2. Особливості встановлення та налаштування параметрів операційної системи за допомогою OracleVBox.

3. Призначення основних програмних компонентів операційної системи Windows щодо адміністрування її роботи.

4. Характеристика програмного забезпечення операційної системи Windows щодо віддаленого адміністрування.

5. Призначення «Журналу подій» операційної системи Windows, призначення журналів, за допомогою яких здійснюється моніторинг роботи.

Лабораторна робота №2

Перевірка стану служб операційного середовища Windows

Метою роботи є вивчення та відпрацювання слухачами послідовності виконання технологічних операцій з перевірки переліку та стану працездатності служб операційної системи Windows (далі – OC) та порядку проведення моніторингу завантаженості операційної системи. Операції, що виконуються, здійснюються під обліковим записом адміністратор системи.

Технічне забезпечення занять

4. Персональне робоче місце студента (ПЕОМ) зі встановленим загальносистемним програмним забезпеченням (OC Windows)

5. Програмне забезпечення віртуалізації OracleVBox.

6. Спеціалізоване програмне забезпечення MS Office., версії ОС Windows.

Питання, що відпрацьовуються на занятті

- 4. Перевірка переліку та стану працездатності служб ОС Windows.
- 5. Моніторинг завантаженості операційної системи Windows.
- 6. Визначення розміру файлу підкачки ОС Windows.

Приклад виконання завдань:

1. Перевірка переліку та стану працездатності служб ОС на прикладі вузла ВМР.

1.1. Запустити програмне забезпечення **OracleVBox** з OC Windows. На робочому столі операційної системи за допомогою лівою кнопки миші активізувати ярлик «**Мой комп'ютер**», далі натиснути на праву кнопку миші. У контекстному меню за допомогою лівої кнопки миші вибрати команду «**Управление**» (рис. 1).

Мои					
кументы					
and the second s					
Мой	F				
мпьютер	Открыть				
	Проводник				
	Найти				
et e	Упраеление				
сетевое	shipdosterine				
S ACTINC	Подключить сетевой диск				
	Отключить сетевой диск				
ODDINNO	Создать ярлык				
oponna	Переименовать				
-	Coolicator				
13 -	Своиства				
-					
nternet					
xplorer					
Пуск	😭 🥔 🕅 🗌 🖼 Администриро	вание 💷 Управление комп	Сеть и удаленны	12.bmp - Paint	EN 50 PR 11
				Contraction of the second seco	

Рис 1. Виклик вікна «Управління комп'ютером»

1.2. У вікні «Управление компьютером» за допомогою лівої кнопки миші активізувати розділ «Службы и приложения», далі «Службы» (рис.2).

📮 Управление компьютером					_ 8 ×
] Действие Вид 🗍 🗢 🔿 🗈 🔃					
Структура	Имя 🔺	Описание	Состояние	Тип запуска	Вход в систему 🔺
Действие Вид Структура травление компьютером (локальным) Служебные программы Служебные программы Сведения о системе Оповещения и журналы производите Общие папки Общие папки Общие папки Общие папки Общие палки Общие палки Общие палки Общие паки Общие паки Общие паки Общие паки Общие паки Общие паки Общие паки Общие паки Сружбы и приложения Службы и приложения Службы и приложения Службы индексирования Службы индексирования Службы индексирования ОК	 Иня Иня Алиспетчер логических дисков Аиспетчер очереди печати Аиспетчер очереди печати Аиспетчер сетевого DDE Аиспетчер сетевого DDE Аиспетчер сетевого DDE Аиспетчер сужебных програми Аиспетчер учетных записей безопас Журнал событий Защищенное хранилище Инструментарий управления Windows Источник бесперебойного питания Клиент отслеживания изменившихся Координатор распределенных транз Покатор удаленного вызова процед Общий доступ к подключению Инте Общий доступ к подключению Инте Оповещатель Оповещения и журналы производит Планировщик заданий Поставщик поддержки безопасност Расширения драйвера оснастки упра Сервер отслеживания изменившихся 	Описание Служба Загруж Создае Управл Обеспе Яаписы Обеспе Предос Управл Посыла Поддер Обеспе Поддер Обеспе Посыла Посыла Посыла Посвила Обеспе Обеспе Обеспе Обеспе Обеспе Обеспе Обеспе Обеспе	Состояние Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает Работает	Тип запуска Авто Авто Авто Вручную Вручную Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто Авто	Bxog в систему LocalSystem LocalSystem
۲	Карана Сервер папки обмена	Позвол	5.6	Вручную •	LocalSystem
	правление компьютером 🔲 Управление	компьют			

Рис. 2. Виклик вікна «Службы»

1.3. Перевірити перелік, стан завантаження та тип запуску служб операційної системи Windows. Під час перевірки стану служб, особливо звернути увагу на запуск служб, які забезпечують працездатність спеціалізованого програмного забезпечення та бази даних.

1.4. У разі необхідності можливо перевірити наявність та стан запуску служб за допомогою командного рядку операційної системи. Для цього натиснути на кнопку **«Пуск»** панелі задач ОС, далі вибрати команду **«Выполнить»** та ввести у командному рядку команду **«стис)** (рис. 4) далі **«ОК»**.

Запуск пр	ограммы	? 🗙
	Введите имя программы, папки, документа I ресурса Интернета, и Windows откроет их.	или
Открыть:	cmd	~
	ОК Отмена Обз	юр

Рис. 4. Запуск команди «сmd»

1.5. У вікні, що з'явиться (рис. 5), ввести в командному рядку команду «net start».



Рис. 5. Запуск команди «net start»

1.6. Виконати перегляд служб, які завантажені та знаходяться у працездатному стані (рис. 6).



Рис 6. Вікно перегляду служб, що завантажені

1.7. У разі виявлення порушень щодо функціонування служб операційної системи, здійснити додаткові заходи з приведення служб операційної системи до працездатного стану або їх перезавантаження, для цього у вікні «Управление компьютером» на правої половині вікна необхідно активізувати лівою кнопкою миші службу та натиснути на кнопку «Запуск службы» або «Перезапуск службы» (рис 7).

	докунс	nn.bac		COU	эвни
🖵 Управление компьютером					×
📙 действие вид 🗍 🖙 🔿 🗈 🔃	🖻 🗗 🖪 😫				
Структура	Имя 🛆	Запуск службы	Описание	Состояние	<u>.</u>
 Управление компьютером (локальным Служебные программы Просмотр событий Сведения о системе Оповещения и журналы произа Общие папки Диспетчер устройств Локальные пользователи и гру Запоминающие устройства Управление дисками Дефрагментация диска Логические диски Съемные ЗУ Службы Телефония Управляющий элемент WMI Службы Службы Докуртизация и удаленный д 	AgentService DHCP-клиент DNS-клиент DNS-сервер Hippo Protocol serv Languard OracleHOME1Ageni OracleHOME1Client OracleHOME1Client OracleHOME1Pagin OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleHOME1SNMP OracleServiceM803 OracleServiceM803 OracleServiceM803 Plug and Play	vice e Desktop Sharing t :Cache Server gServer PeerEncapsulator PeerMasterAgent istener yService 14 19 0	Управляе Разрешае Отвечает Разрешае Управляе Обеспечи	Работает Работает Работает Работает Работает Работает Работает Работает	×

Рис 7. Порядок запуску служби

1.8. За результатами робіт зробити остаточний висновок щодо наявності та стану працездатності програмних служб ОС ПЕОМ.

2. Моніторинг завантаженості операційної системи Windows

2.1. Контроль за станом пам'яті ПЕОМ.

2.1.1. Послідовно за допомогою програмного забезпечення **OracleVBox** навчального класу перевірити параметри пам'яті OC, а саме:

- розмір фізичної оперативної пам'яті, що виділяється;

- загальний розмір пам'яті, яку на даний час займають всі процеси, що використовуються ОС.

Для цього запустити на однієї з віртуальних машин програмне забезпечення «**Диспетчер задач Windows**» та протягом 20-30 хвилин здійснити аналіз параметрів пам'яті, які використовує операційна система (рис.1).

2.1.2. На приклад, під час роботи видно, що розмір фізичної оперативної пам'яті, виділений ОС складає **785904 Кб**, загальний розмір пам'яті, яку на даний час займають всі процеси ОС – **450392 Кб** (рис.1).

2.1.3. Перевірити розмір файлу підкачки оперативної пам'яті ОС, для цього лівою кнопкою миші активізувати значок «Мой компьютер», далі натиснути на праву кнопку миші та вибрати «Свойства». У вікні, що з'явиться вибрати закладку «Дополнительно», «Параметры», далі закладку «Дополнительно».

В розділі віртуальної пам'яті визначити розмір файлу підкачки, що встановлюється для роботи ОС (рис.2.). На прикладі роботи видно, що розмір файлу підкачки складає **1152** Мб, що приблизно в **1,5 рази більше** розміру встановленої фізичної пам'яті.

2.1.4. Визначити розмір пам'яті, що використовують програми (процеси), які запущені на віртуальної машині (рис.3).

Для цього у вікні «Диспетчера задач» необхідно активізувати закладку «Процессы» (рис.3) та прослідкувати за станом зміни розміру пам'яті, що використовують програми які запущені.

Якщо протягом тривалого часу, програма коректна не звільняє пам'ять, що виділяється для неї, а її робочий простір постійно збільшується, це означає, що програма працює некоректно. У таких випадках погіршується продуктивність роботи ОС та збільшується її завантаженість.

📕 Диспетчер за,	дач Windows		
Файл Параметры	Вид Справка		
Приложения Пр	оцессы Быстроде	йствие Сеть	
_ Загрузка ЦП -	Хронология з	агрузки ЦП	
16 %			
Файл подкачк	и Хронология и	использования файла	подкачки
439 MB			
Bcero		🖓 Физическая память	(КБ)
Дескрипторов	10345	Всего	785904
Потоков	350	Доступно	276880
Процессов	30	Системный кэш	315544
-Выделение па	мяти (КБ)	_Память ядра (КБ) -	
Bcero	450392	Всего	31244
Предел	1923368	Выгружаемая	25632
Пик	536476	Невыгружаемая	5612
Процессов: 30	Загрузка ЦП: 16%	Выделение памят	и: 439МБ / 6

Рис.1. Від вікна Диспетчера задач Windows



Рис.2. Визначення розміру файлу підкачки OC Windows

В , Фай	ци <mark>спетчер задач</mark> У іл Параметры Вид	Vindows Справка			_ 🗆	×
Пр	иложения Процесси	ы Быстродействие	Сеть	1		
	Имя образа	Имя пользователя	ЦП	Память		
	oracle.exe	SYSTEM	01	271 216 КБ		
	TNSLSNR.EXE	SYSTEM	00	7 556 KB		
	java.exe	administrator	00	20 128 КБ		
	java.exe	SYSTEM	01	44 360 KE		
	taskmgr.exe	administrator	01	1 696 KB		
	svchost.exe	SYSTEM	00	3 832 КБ		
	alg.exe	LOCAL SERVICE	00	З 136 КБ		
	vpcmap.exe	SYSTEM	00	916 KB		

Рис.3. Від вікна щодо запущених процесів ОС Windows

2.1.5. Виконати заходи щодо усунення некоректної роботи програми шляхом її перезапуску. Якщо у подальшому витяг пам'яті для процесу (програми) продовжується, повідомити про це викладачу.

3. Визначення розміру файлу підкачки ОС Windows

3.1. Перевірити розмір файлу підкачки ОС на віртуальної машині.

За рекомендаціями фірми Microsoft розмір файлу підкачки підраховується за наступною формулою: **FP*1,5**, де **FP** – розмір фізичної пам'яті (**M6**). Для віртуальної машини, наведеного у прикладі, розмір файлу підкачки складає 785*1,5 = 1177**M6**, що приблизно співпадає з існуючим його розміром (1152 **M6**).

3.2. Зазначений метод використовується у випадках малої фізичної пам'яті, якщо фізичної пам'яті більше, то розмір файлу підкачки потрібно встановлювати меншим.

3.3. Для виконання операцій зміну розміру файлу підкачки необхідно на панелі задач операційної системи віртуальної машині натиснути на кнопку «Пуск», далі «Настройка», «Панель управления», «Администрирование», вибрати «Производительность». У вікні «Производительность», активізувати розділ «Системный монитор» (рис.4).

3.4. На панелі інструментів вікна «Системный мониторинг» натиснути на кнопку «Добавить», яка має позначку «+», далі у полі з назвою «Объект» вибрати «Файл подкачки» та активізувати лічильник «% использования», далі натиснути на кнопку «Добавить», після чого на кнопку «Закрыть» (рис.5).

3.5. Протягом певного часу прослідкувати за використанням файлу подкачки (рис.6), після чого у вікні «Системный мониторинг» натиснути на кнопку «Просмотр отчета» та здійснити підрахунок відсотка використання файлу підкачки та визначити його середній розмір у % (рис.7).

3.6. Наприклад, при пікових навантаженнях, відсоток використання файлу підкачки складає 40, 28, 36 и 30 середнє значення завантаженості складає 34.5%. Якщо раніше файл підкачки був встановлений 1152 Мб то приймаємо зазначений показник за 100%, далі підрахуємо його остаточний розмір: 1152:100*34.5%=2*34.5%=приблизно 398MB. Якщо додати до визначеного розміру 20M6 (враховуючі максимальний пик навантаження) то остаточний розмір файлу буде 418M6.

Примітка: Включення лічильників на віртуальної машині може сприяти погіршенню на деякій час продуктивності програмних компонентів ОС.

👿 Производительность	
📷 Консоль Действие Вид Изб	іранное Окно Справка
Корень консоли Системный монитор	📋 🖓 Ə 🔛 🖬 🕂 🗙 🛊 🛍 😂 🛎 🔮
표 🎆 Журналы и оповещения прог	100
	80
	60
	40
	20
	Последний 0,000 Средний 2,830
	Минимум 0,000 Максимум 200,990
	Длительность 1:40
	Цвет Шк Счетчик Экземп Роди Объект Компьютер
	1,000 Обмен стра Память \\WAP00M8
	100, Средняя длTotal Физич \\WAP00M8
< >	1,000 % загружен1осан Проце \\WAP00M8

Добавить счетчики	<u>? ×</u>
 Использовать локальные счетчики Выбрать счетчики с компьютера: \\ORACL 	
Объект:	
Файл подкачки	
О Все счетчики	Все вхождения
Выбрать счетчики из списка	Выбрать вхождения из списка:
% использования % использования (пик)	\??\C:\pagefile.sys _Total
Добавить Объяснение	





3.7. Після закінчення робіт здійснити заходи з віддалення лічильника «% использования». Для цього у вікні «Системный мониторинг» на правій половині вікна активізувати лівою кнопкою миші лічильник «% использования», далі натиснути на кнопку «Удалить», яка має позначення «Х».

Завдання на виконання лабораторної роботи

1. Перевірити встановлення програмного забезпечення **OracleVBox** на робочому місці студента та здійснити в разі необхідності його налаштування.

2. Встановити на віртуальну машину одну з версій операційної системи (Windows 10, Windows 7, Windows XP). Версію ОС студенту призначає викладач.

3. Перевірити працездатність зв'язку між операційною системою, встановленою на віртуальної машині та операційною системою ПЕОМ робочого місця студента. за допомогою **OracleVBox.**

4. Здійснити перевірку переліку та стану працездатності служб ОС Windows віртуальної машини.

5. За допомогою «Диспетчера задач Windows» виконати моніторинг завантаженості операційної системи Windows віртуальної машини.

6. Здійснити розрахунок розміру файлу підкачки OC Windows.

7. За результатами робіт підготувати звіт щодо завантаженості операційної системи Windows.

ЗРАЗОК ЗВІТУ

N⁰	розмір фізичної	загальний	розмір	відсоток
3.П.	оперативної	розмір пам'яті	файлу	використання
	пам'яті		підкачки	файлу підкачки
				під час пікових
				навантажень

Контрольні питання (відповісти письмово)

1. Призначення, характеристика програмного забезпечення OracleVBox.

2. Особливості встановлення та налаштування параметрів операційної системи за допомогою OracleVBox.

3. Основні служби операційної системи Windows, їх призначення та способи запуска.

4. Характеристика програмного забезпечення операційної системи Windows щодо визначення завантаженості її роботи.

5. Призначення «Диспечера задач» операційної системи Windows, характеристика показників, за допомогою яких здійснюється моніторинг роботи.

6. Методика визначення розміру файлу підкачки ОС Windows

Лабораторна робота №3

Моніторинг операційної системи за допомогою програмного забезпечення Performance Monitor

Метою роботи є перевірка параметрів (характеристик) складових ОС, розміру та витоку пам'яті, працездатності процесора, оцінку впливу параметрів налаштування на роботу ОС. У роботі виконується контроль інших параметрів, що впливають на завантаженість роботи ОС, зокрема, характеристик роботи твердих магнітних дисків.

Контроль за параметрами пам'яті та процесора здійснюється як на етапі начальної загрузки ПЕОМ, так і під час її тривалої роботи.

Технічне забезпечення занять

1. Персональне робоче місце студента (ПЕОМ) зі встановленим загальносистемним програмним забезпеченням (ОС Windows)

2. Програмне забезпечення віртуалізації OracleVBox.

3. Спеціалізоване програмне забезпечення MS Office., версії ОС Windows.

Питання, що відпрацьовуються на занятті

1. Контроль за станом завантаженості процесора на ПЕОМ.

2. Контроль за станом завантаженості OC Windows за допомогою програмної утиліти msconfig.exe.

3. Моніторинг завантаженості операційної системи за допомогою програмного забезпечення «Performance Monitor»

Приклад виконання завдань :

1. Контроль за станом завантаженості процесора на ПЕОМ

1.1. Перевірити ступень завантаженості процесора прикладними програмами або процесами, що використовує операційна система на віртуальної машині. Особливо необхідно проконтролювати те процеси, що знаходяться в циклі очікування. Такі процеси в окремих випадках створюють сто відсоткову завантаженість процесора, але не заважають роботу ПЕОМ.

1.2. Виконати перевірку загальної завантаженості процесора за допомогою вікна «Диспечер задач». Для цього проаналізувати стовпчик на закладці «Процессы» справа від назви процесів, що працюють «ЦП». Цей стовпчик показує скільки відсотків від загальної завантаженості процесора займає кожний процес окремо. (рис.3.).

1.3. Якщо під час перевірки з'ясовано, що процес займає значну частину ресурсу (наприклад більше 30%), то він є причиною повільної роботи операційної системи. Причина зависання ОС Windows може буде з'ясована за результатами огляду стовпчику «Память», а саме, за кількістю пам'яті, що використовує кожний процес.

1.4. Для усунення зависання ОС необхідно активізувати програму (процес), що заважає роботі, далі натиснути на праву кнопку миші, у контекстному меню вибрати команду «Завершить процесс», далі натиснути на кнопку «Да» (рис.1).

1	svenose.e	exe	SYSTEM	00	5	3 820 KB	
1	alg.exe		LOCAL SERVICE	- 00	0	3 136 КБ	
- t	taskmgr.(exe	administrator	- 01	1	3 336 KE	
. I .	vpcmap.e	exe	SYSTEM	- 00	D	916 KB	
1	locator.e	xe	NETWORK SERVICE	- 00	D	2 312 КБ	
	ctfmon.e	xe	administrator	- 00	D	2 704 КБ	
- I -	vmusrvc.	exe	administrator	- 00	D	2 536 KB	
l I	nmesrvc.	exe	SYSTEM	- 00	D	1 124 КБ	
	explorer.	exe	administrator	- 00	D	21 332 КБ	
. I I	vmsrvc.e	xe	SYSTEM	- 00	D	1 916 KB	
	perl.e	_		- 00	0	7 588 KB	
Ī	cmd.e	Завершить	процесс	00)	1 220 KB	
1	spools	Завершить	дерево процессов	00	D	4 380 KE	
1	svcho	Отладка		00	D	4 664 KB	
	emagi —			— D O	D	18 332 KB	
:	svcho	Приоритет		• 00	D	2 624 КБ	
	sycho st e	ave	SYSTEM		٦	17 684 KE	_
Γ	Отобр	ажать проц	ессы всех пользова	телей	í	Завершить про	цесс

Рис.1. Відключення процесів, що заважають роботі ОС

2. Контроль за станом завантаженості OC Windows віртуальної машини за допомогою команди msconfig.exe

2.1 Натиснути на кнопку «Пуск» панелі задач ОС на віртуальної машині, далі необхідно вибрати кнопку «Выполнить», у вікні, що з'явиться набрати команду msconfig.exe (рис.2). У вікні, що з'явиться активізувати закладку «Атозагрузка» (рис.3).

Запуск программы
Введите имя программы, папки, документа или ресурса Интернета, и Windows откроет их.
Открыть: msconfig
ОК Отмена Обзор

Рис.2. Запуск команди msconfig.exe

2.2. Перевірити перелік програм, що завантажуються разом з ОС. Якщо під час перевірки виявлено програми, які не повинні бути автоматично запущені на етапі начальної загрузки ОС, то виконати їх зупинку шляхом видалення мітки, що встановлена проти відповідної програми (рис.3).

3. Моніторинг завантаженості операційної системи за допомогою програмного забезпечення «Performance Monitor»

3.1. Здійснити запуск програмного забезпечення «**Performance Monitor**» на віртуальної машині. Враховуючи пропозиції, що наведені у таблиці визначити необхідні лічильники, що будуть використовуватися протягом виконання операцій з моніторингу завантаження ОС.

📕 Настройка системы			×
Общие SYSTEM.INI WIN	І.INI ВООТ.INI Службы	Автозагрузка	. 1
Элемент автозагрузки	Команда	Расположение	
Vmusrvc	C:\Program Files\Virtu	HKLM\SOFTWARE\Microsoft\Windows\CurrentVer	
🗹 bckp7	e:\vti\utils\bckp\bckp7	HKLM\SOFTWARE\Microsoft\Windows\CurrentVer	
Ctfmon	C:\WINDOWS\system	HKCU\SOFTWARE\Microsoft\Windows\CurrentVer	

Рис.3. Відключення автозавантаження програм ОС

3.2. На протязі 20 хвилин навчального часу здійснити підрахунок необхідних характеристик завантаженості пам'яті та процесору OC Windows віртуальної машини. Назва лічильників та об'єкти, що вони контролюють, надаються у таблиці.

Примітка: Назва лічильників OC Windows у залежності від версії може бути іншою.

Об'єкт: Лічильник	Призначення
(Процесор: Робоче	Кількість фізичної оперативної пам'яті, що
середовище)	використовується процесором
(Процесор: Байт файлу	Кількість пам'яті, що процес використовує у файлі
підкачки)	підкачки.
(Память: Байт	Загальний розмір віртуальної пам'яті, яку на даний час
віртуальної пам'яті)	займають всі процеси користувачів.
(Память: Предел	Величина, яка визначає кількість віртуальної пам'яті
віртуальної пам'яті	система може надати без збільшення розміру файла
	підкачки.
(Процесор: %	Ступень використання процесора заданим процесом.
завантаженості	
процесора)	

Таблиця - Назва та призначення основних лічильників Performance Monitor

3.3 Після закінчення робіт здійснити заходи з віддалення лічильників. Для цього у вікні «Системный мониторинг» на правій половині вікна активізувати лівою кнопкою миші необхідний лічильник, далі натиснути на кнопку «Удалить», яка має позначення «Х» далі натиснути на кнопку «Удалить», яка має позначення «Х».

Завдання на виконання лабораторної роботи

1. Перевірити працездатність операційної системи Windows на віртуальної машині за допомогою програмного забезпечення **OracleVBox**, у разі необхідності здійснити налаштування її роботи.

2. Виконати моніторинг завантаженості операційної системи за допомогою програмного забезпечення «**Performance Monitor**»

3. За результатами робіт підготувати звіт.

ЗРАЗОК ЗЕ	ЫТУ
------------------	-----

Об'єкт перевірки	Одиниця	Середнє значення
	вимірювання	параметру
Кількість фізичної оперативної		
пам'яті, що використовується		
процесором		
Кількість пам'яті, що процес		
використовує у файлі підкачки.		
Загальний розмір віртуальної		
пам'яті, яку на даний час займають		
всі процеси користувачів.		
Величина, яка визначає кількість		
віртуальної пам'яті система може		
надати без збільшення розміру		
файла підкачки.		
Ступень використання процесора		
заданим процесом.		

Примітка: Назва лічильників у залежності від версії операційної системи може змінюватися

Контрольні питання (відповісти письмово)

1. Призначення, характеристика програмного забезпечення «Performance Monitor»

2. Програмні утілити операційної системи Windows щодо перевірки завантаженості її роботи.

3. Призначення, назва лічильників, що використовуються для перевірки роботи компонентів операційної системи Windows.

4. Призначення, назва лічильників, що використовуються для перевірки роботи обладнання ПЕОМ.

5. Навести приклади та короткий опис інших програмних утиліт щодо перевірки завантаженості та перевірки роботи програмного та апаратного забезпечення операційної системи Windows.
Лабораторна робота №4

Перегляд журналів подій та системного журналу безпеки операційної системи Windows

Метою роботи є відпрацювання завдань щодо порядку перегляду та перевірки вмісту подій, що виникають під час експлуатації загальносистемного та прикладного програмного забезпечення на ПЕОМ користувача та сервера за допомогою журналів подій та системного журналу безпеки операційної системи Windows.

Технічне забезпечення занять

1. Персональне робоче місце студента (ПЕОМ) зі встановленим загальносистемним програмним забезпеченням (ОС Windows)

2. Програмне забезпечення віртуалізації OracleVBox.

3. Спеціалізоване програмне забезпечення MS Office., версія OC Windows 7/10 та версія OC Window Server 2012/2016.

4. Програмне забезпечення контролеру домену ОС Window Server 2012/2016.

Питання, що відпрацьовуються на занятті

1. Перегляд подій у журналах подій операційної системи.

2. Перевірка характеру подій у журналі безпеки операційної системи

3. Перевірка розміру журналів подій, їх аналіз та очищення.

Порядок виконання завдань:

1. Перегляд та перевірка характеру подій у журналах подій ОС.

1.1. Послідовно за допомогою облікового запису «Администратор» здійснити перегляд журналів подій операційної системи Windows на ПЕОМ слухача на сервері навчального класу. Для цього на робочу столі операційної системи ПЕОМ за допомогою лівої кнопки миші активізувати значок «Мой копьютер», натиснути на праву кнопку миші, далі «Управление», у вікні, що з'явиться, вибрати «Просмотр событий» та відповідний журнал подій:

на ПЕОМ користувачів (рис1):

- додатків;
- системи.

Ц К	у Консоль Действие Вид Окно Справка							
¢	→ 🖻 🖬 📽 🖗 😫	?						
<mark>.</mark>	правление компьютером (локаль	Тип	Дата	Время	Источник	Категория	Соб	Пользова
- E - 👔	🔓 Служебные программы	Уведомление	07.12.2009	9:11:26	ESENT	Общие	101	Н/Д
E	🛙 🜆 Просмотр событий	ФУведомление	07.12.2009	9:11:26	ESENT	Общие	103	Н/Д
	Приложение	ЭУведомление	07.12.2009	9:06:15	ESENT	Общие	102	Н/Д
	и система	Уведомление	07.12.2009	9:06:15	ESENT	Общие	100	Н/Д
	Побщие папки	Уведомление	07.12.2009	9:05:28	SPIDERNT	Отсутст	13	Н/Д
	Покальные пользователи и	🔥 Предупре	04.12.2009	18:12:39	Userenv	Отсутст	1517	SYSTEM
	🛛 🐺 Журналы и оповещения пр	Уведомление	04.12.2009	9:05:44	ESENT	Общие	101	Н/Д
	🛄 Диспетчер устройств	Уведомление	04.12.2009	9:05:44	ESENT	Общие	103	Н/Д
÷-8	Запоминающие устройства	Уведомление	04.12.2009	9:00:40	ESENT	Общие	102	Н/Д
	A CLAMULIA RV	I 🥲 Уведомление	04.12.2009	9:00:40	ESENT	Обшие	100	H/Д

Рис.1. Вигляд вікна перегляду журналів подій на ПЕОМ

на сервері (рис.2.):

- додатків;
- Directory Service;
- DNS Server;
- служба реплікації файлів;
- система

] Действие вид] 🗢 ⇒ 🔁	1 🖬 🔮 🚱	2						
Структура	Тип	Дата	Время	Источник	Категория	Соб	Пользователь	Компьютер
Управление компьютером (локаль	ным 🔥 Предупре	07.12.2009	10:02:11	WinMgmt	Отсутст	61	Нет данных	SPN00X00
🗄 🐔 Служебные программы	🔅 Уведомления	07.12.2009	10:01:21	SceCli	Отсутст	1704	Нет данных	SPN00X00
🖻 🛐 Просмотр событий	Уведомления	07.12.2009	10:01:12	ESENT	Общие	101	Нет данных	SPN00X00
	😣 Ошибка	07.12.2009	10:01:11	CertSvc	Отсутст	100	Нет данных	SPN00X00
- 🔢 Directory Service	😣 Ошибка	07.12.2009	10:01:10	CertSvc	Отсутст	58	Нет данных	SPN00X00
DNS Server	😣 Ошибка	07.12.2009	10:01:09	FtpCtrs	Отсутст	1000	Нет данных	SPN00X00
📔 🦳 🛄 Служба репликации фа	айлов 😲 уведомления	07.12.2009	10:01:04	ESENT	Общие	100	Нет данных	SPN00X00
Безопасность	🔅 Уведомления	07.12.2009	10:00:48	EvntAgnt	Отсутст	2018	Нет данных	SPN00X00
📕 Система	🔅 Уведомления	07.12.2009	10:00:37	ESENT	Общие	100	Нет данных	SPN00X00
🕀 📲 Сведения о системе	(і) Уведомления	07.12.2009	10:00:33	ESENT	Общие	100	Нет данных	SPN00X00

Рис.2. Вигляд вікна перегляду журналів подій на сервері

1.2. Перевірити записи у зазначених журналах та здійснити перегляд номерів повідомлень, які мають тип записи «Ошибка» або «Предупреждение».

Для цього необхідно активізувати відповідний запис у журналі та два рази натиснути на ліву клавішу миші. У вікні, що з'явиться, здійснити перегляд вмісту повідомлення. (рис.3).



Рис.3. Перегляд вмісту події за допомогою журналу DNS Server

1.3. При появи помилок або попереджень з'ясувати причину їх появи та прийняти рішення щодо подальшого продовження роботи ПЕОМ та сервера.

2. Перевірка характеру подій у журналі безпеки ОС.

2.1. Перевірити встановлення та налаштування політик аудиту на сервері, якщо сервер налаштований як контролер домену. Для цього на панелі контролера домену вибрати **«Локальные политики»** та відкрити оснастку **«Політика аудиту».** Здійснити огляд встановлених параметрів аудиту (рис.4.)

🚰 Политика безопасности домена						
] Действие вид 🛛 🖛 🔿 🗈 💽 🗙	B 2					
Структура	Политика 🔺	Параметр компьютера				
🦲 Конфигурация Windows	🕮 Аудит входа в систему	Успех, Отказ				
🗄 🔂 Параметры безопасности	📖 Аудит доступа к объектам	Успех, Отказ				
🗄 🛃 Политики учетных записей	闘 Аудит доступа к службе каталогов	Не задан				
🗄 🖟 🛃 Локальные политики	👸 Аудит изменения политики	Не задан				
— 🛃 Политика аудита	闘 Аудит использования привилегий	Не задан				
🕀 👮 Назначение прав пользователя	闘 Аудит отслеживания процессов	Не задан				
🗄 🚮 Параметры безопасности	📖 Аудит системных событий	Не задан				

Рис.4. Перевірка налаштувань політик аудиту на сервері

2.2. Послідовно виконати аналіз журналів безпеки ОС на робочої станції користувача. Для цього на робочому столі операційної системи користувача активізувати лівою кнопкою миші значок «Мой копьютер», далі натиснути на праву кнопку миші, у контекстному меню вибрати «Управление» та натиснути на ліву кнопку миші, у вікні, що з'явиться вибрати «Просмотр событий» далі «Безопасность» (рис.5).

Структура	Тип	Дата	Время	Источник	Категория	Соб	Пользователь
Управление компьютером (локальным)	💰 Аудит усп	09.12.2009	14:40:35	Security	Доступ	562	SYSTEM
🗐 🐔 Служебные программы	🥑 Аудит усп	09.12.2009	14:40:35	Security	Изменен	612	SYSTEM
🖻 🔞 Просмотр событий	🥑 Аудит усп	09.12.2009	14:40:35	Security	Доступ	562	SYSTEM
Приложение	🥑 Аудит усп	09.12.2009	14:40:35	Security	Доступ	560	SYSTEM
— 🕖 Безопасность	🥑 Аудит усп	09.12.2009	14:40:35	Security	Доступ	560	SYSTEM
Система	🥑 Аудит усп	09.12.2009	14:40:34	Security	Вход/вы	538	SYSTEM
🕀 🖳 Сведения о системе	🥑 Аудит усп	09.12.2009	14:40:33	Security	Вход/вы	540	SYSTEM
🕀 🎆 Оповещения и журналы произе	🥑 Аудит усп	09.12.2009	14:40:24	Security	Доступ	562	SYSTEM
🗄 🖾 🥅 Общие перии	I <u>4</u> .		· · · ·		-		

Рис.5. Перегляд типу подій в журналі безпеки ОС

2.3. Згідно п. 1.2. виконати аналіз вмісту повідомлень, які відображені у журналі безпеки користувача (рис.6), особливо щодо подій, які зазначені у таблиці.

Таблиця – Приклад номерів подій журналу безпеки ОС, які потребують перегляду

№ події	Короткий зміст (мовою операційної системи)					
528	Успешный вход в систему					
529	Отказ входа в систему. Неизвестное имя пользователя					
530	Пользователь пытался войти в систему в					
	недозволенное ему время					
531	Учетная зпись пользователя заблокирована					
532	Учетная запись пользователя просрочена или устарел					
	пароль пользователя.					
533	Пользователь ограничен входом лишь на некоторые					
	рабочие станции, а он пытается войти в систему с другого					
	компьютера					
534	Попытка запуска службы с использованием учетной					
	записи пользователя, не имеющей права на запуск служб					
537	Отказ по неизвестной причине					
538	Выход пользователя из системы					
540	Успешный сетевой вход в систему					
560	Фиксирует открытия объекта пользователем					
562	Фиксирует закрытия объекта пользователем					
628	Задание пароля учетной записи					
642	Изменение учетной записи					
644	Блокировка учетной записи пользователя в домени					

та контролю

Примітка: В залежності від версії ОС № подій може відрізнятися.

ι	воиства:	соовние			<u> </u>
	Событие				
	Дата: И Время: 1 Тип: / Пользов Компью	09.12.2009 14:40 Аудит успехов затель: <u>NTAU</u> тер: WAP00 не:	Источник: Категория: Код (ID): <mark>THORITY\SY</mark> IM8000	Security Вход/выход 538 <mark>STEM</mark>	 ↑ ↓ □
	Выход г	юльзователя и Пользовател Домен: Код входа: Тип входа:	з системы: ь: WAPOC M8040I (0x0,0x 3)M8000\$ R80 2CCC0)	

Рис.6. Перегляд події в журналі безпеки користувача

2.4. Перевірити записи в журналі безпеки ОС користувача щодо подій, пов'язаних з реєстрацією користувача, а саме, визначити номер типу входу користувача в систему.

В журналі безпеки зазначені події фіксуються наступними порядковими номерами:

2 – відповідає інтерактивному входу в систему з консолі, наприклад за допомогою монітору або клавіатури;

3 – підключення до системи за допомогою мережевого ресурсу;

4 – вказує на запуск командного файлу;

5 – фіксує запуск служби з зазначенням облікової записі користувача

6 – підключення користувача здійснюється за допомогою Proxy Server

7 – користувач здійснював розблокування робочої станції.

Якщо під час аналізу були виявлені спроби несанкціонованого доступу (реєстрації) користувачів (події №№529, 530, 537, тип входу 2,3), необхідно ретельно проаналізувати зазначені події та прийняти заходи щодо недопущення несанкціонованого доступу до ресурсів ПЕОМ.(рис.7)



Рис.7. Перегляд події в журналі безпеки щодо спроби несанкціонованого

доступу на ПЕОМ користувача

2.5. Здійснити аналіз подій журналу безпеки щодо доступу користувача до об'єктів системи (події за номерами 560 та 562 рис. 8.). До таких об'єктів відносяться виконавчі файли загальносистемного та прикладного програмного забезпечення (програмне забезпечення ПЕОМ, клієнтське програмне забезпечення СКБД, Microsoft Office тощо).

За результатами розгляду проаналізувати коректність доступу користувачів до зазначеного програмного забезпечення.

Событие			
Дата: 09.12.2009 Время: 14:40 Тип: Аудит успехов Пользователь: <mark>NT AUT</mark> Компьютер: WAP00	Источник: Категория: Код (ID): <mark>(HORITY\SYS</mark> M8000	Security Доступ к объектам 560 <mark>ЭТЕМ</mark>	 ↑ ↓ ↓
Описание:	пьзователь: ь-клиент: та: иента: DELETE	WAPUUM8UUU\$ M8040R80 (0x0,0x3E7) WAP00M8000\$ M8040R80 (0x0,0x3E7)	

Рис.8. Перегляд події в журналі безпеки щодо доступу до прикладного програмного забезпечення користувача

3. Перевірка налаштувань журналів подій та безпеки ОС

3.1. На віртуальної машині користувача або сервера відрити вікно «Управление компьютером», за допомогою лівої кнопки миші вибрати розділ «Просмотр событий», далі активізувати необхідний журнал подій ОС, натиснути на праву кнопку миші та у контекстному меню вибрати команду «Свойства» (рис.9).

управление ког	пьютером (локаль Тип	Дата
- 🌇 Служебные	программы	
🚊 🔞 Просмот	р событий	
Torr		
🛛 🙀 Бе	Открыть файл журнала	
Си	Сохранить файл журнала как	
🗄 💫 Общие	Создать вид журнала	
🕀 🚮 Локал	Стереть все события	
😟 🎆 Журна 🗌		
🔤 🔜 Диспе _	повое окно отсюда	
🛬 Запоминан	Переименовать	
🗄 🔗 Съемн	Обновить	
🛛 🥵 Дефра 🔤		-
🖓 Управ	Свойства	
🌆 Службы и 🗌	Справка	
— 🦓 Служб	Chpabita	

Рис.9. Вибір вікна властивостей журналу подій

3.2. Перевірити значення конфігураційних параметрів журналу, а саме, його максимальний розмір та правило записи у журнал при його заповненні (затирать события старее 7 дней). За допомогою кнопки «Очистить журнал» здійснити видалення його повідомлень (рис.10).

войства: Приложение 🤶 🔀						
Общие Фильтр	l					
Выводимое имя:	Приложение					
Имя журнала:	C:\WINDOWS\system32\config\AppEvent.Evt	-				
Размер:	Размер: 512,0 КБ (524 288 байт)					
Создан: 16 августа 2009 г. 16:27:41						
Изменен: 14 ноября 2009 г. 0:22:47						
Открыт: 14 ноября 2009 г. 0:22:47						
Размер журнал	Размер журнала					
Максимальны	ий размер журнала: 4096 📑 КБ					
По достижени	и максимального размера журнала:					
О Затирать (старые события по необходимости					
 Затирать 	события старее 7 📑 дней					
С Не затирать события (очистка журнала вручную) Восстановить умолчания						
Подключение по медленной линии Очистить журнал						
	ОК Отмена Примен	нить				

Рис.10 Від вікна налаштувань журналу повідомлень ОС

Завдання на виконання лабораторної роботи

1. Перевірити працездатність операційної системи Windows ПЕОМ користувача на віртуальної машині за допомогою програмного забезпечення **OracleVBox**, у разі необхідності здійснити налаштування її роботи.

2. Перевірити працездатність операційної системи Windows Server користувача на віртуальної машині за допомогою програмного забезпечення OracleVBox.

3. Перевірити працездатність операційної системи Windows Server користувача віртуальної машині у режимі контролеру домену.

4. Перевірити за допомогою утиліти командної строки «**ping**» із зазначенням IP адреси серверу зв'язок між ПЕОМ користувача та контролером домену. (на приклад **ping 192.168.10.6** - де **192.168.10.6** IP адреса сервера.)

5. Виконати приєднання ПЕОМ користувача віртуальної машині до контролеру домену за допомогою обліковій записи «Администратор».

6. Створити засобами контролеру домену новий обліковий запис із зазначенням паролю.

7. Виконати приєднання ПЕОМ користувача віртуальної машині до контролеру домену за допомогою новий обліковій записі.

8. Виконати приєднання ПЕОМ користувача віртуальної машині до контролеру домену за допомогою новий обліковій записі із зазначенням не існуючого паролю.

9. Переглянути події у журналах операційної системи серверу та ПЕОМ користувача віртуальної машини.

10. Перевірити характер подій у журналі безпеки операційної системи серверу.

11. Виконати перевірку розміру журналів подій, та здійснити їх аналіз та очищення.

12. За результатами робіт підготувати звіти.

ЗРАЗОК ЗВІТУ №1

Назва	Опис	Опис	Номер подій	Короткий
журналу ОС	наявних	наявних	журналу	зміст події
	попереджень	критичних	безпеки	журналу
		помилок		безпеки

ЗРАЗОК ЗВІТУ №2

Назва журналу ОС	Встановлений розмір	Адреса розміщення
	журналу	журналу на дисках
		ПЕОМ

Контрольні питання (відповісти письмово)

1. Порядок встановлення та налаштування роботи контролеру домену.

2. Особливості створення обліковій записи користувача за допомогою контролеру домену.

3. Методика перевірки стану зв'язку між контролером домену та ПЕОМ користувача.

4. Назвіть основні журнали операційної системи Windows, за допомогою яких здійснюється моніторинг роботи програмного та апаратного забезпечення ПЕОМ та сервера.

5. Визначити за допомогою технічної документації ОС Windows основні необхідні розміри журналів операційної системи Windows.

6. Опишіть основні правила перевірки та очищення системних журналів операційної системи Windows.

Лабораторна робота №5

Перевірка функціонування та величини завантаження локальної мережі, швидкості та активності роботи контролеру домену

Метою роботи є виконання технологічних операцій з перевірки функціонування та величини завантаження локальної мережі, швидкості та активності роботи контролеру домену на базі операційної системи Windows 2012/2016.

Перевірка функціонування та завантаженості локальної мережі пов'язана перш за все з перевіркою величини завантаження контролеру домену, його програмних складових (Active Directory) та апаратних засобів, що потребують моніторингу та аналізу.

Технічне забезпечення занять

1. Персональне робоче місце студента (ПЕОМ на базі віртуальної машини) зі встановленим загальносистемним програмним забезпеченням (OC Windows)

2. Програмне забезпечення віртуалізації OracleVBox.

3. Спеціалізоване програмне забезпечення MS Office., версія OC Windows 7/10 та версія OC Window Server 2012/2016.

4. Програмне забезпечення контролеру домену ОС Window Server 2012/2016.

Питання, що відпрацьовуються на занятті

1. Перевірка функціонування та величини завантаження локальної мережі.

2. Перевірка величини завантаження контролеру домену на базі ОС Window Server 2012/2016 за допомогою програмного забезпечення «Performance Monitor».

3. Моніторинг роботи Active Directory контролеру домену.

Приклад виконання завдань:

1. Перевірка функціонування та величини завантаження локальної мережі

1.1. Визначити максимальну кількість активних сеансів на контролері домену та здійснити перевірку функціонування локальної мережі та величини її

завантаження. Для цього на панелі задач операційної системи Windows контролера домену вибрати іконку підключення до локальної мережі та натиснути на праву кнопку миші, далі у контекстному меню вибрати команду «Состояние». У вікні, що з'явиться, переглянути стан працездатності мережі, тривалість передачі та кількості отриманих та переданих пакетів (рис.1).

Отключить Состояние Открыть папку "Сеть и удаленнь	лока бит/с паке кето кето	льной сет : :тов в 14:50
		14:50
Состояние Подключение по ло	кальной сети 🤶	2
Общие		
Подключение		
Состояние:	Подключено	
Длительность:	00:18:42	
Скорость:	10.0 Мбит/с	
- Активность	_	
Отправлено —	🕮 — Принято	
Пакетов: 531	409	
Свойства Отключить	1	

Рис.1. Перевірка стану працездатності локальної мережі мережевого

серверу

1.2. Запустити на контролері домену «Диспетчер задач» та здійснити вибір закладки «Сеть» (рис.2). Перевірити стан працездатності мережевого адаптера сервера шляхом визначення відсотка завантаження мережі та швидкості надсилання та отримання мережевих пакетів.



Рис.2. Від вікна «Диспетчер задач»

Примітка: Якщо протягом експлуатації контролеру виникають випадки зупинки надсилання та отримання мережних пакетів або погіршення продуктивності серверу, здійснити додаткові заходи з перевірки стану завантаження мережі за допомогою програмного забезпечення «Performance Monitor».

2. Перевірка величини завантаження мережного сервера за допомогою програмного забезпечення «Performance Monitor».

2.1. На панелі задач операційної системи сервера користувача вузла натиснути на кнопку «Пуск», далі «Настройка», «Панель управления», «Администрирование», вибрати «Производительность». У вікні «Производительность», активізувати розділ «Системный монитор» (рис.3).

2.2. На панелі задач вікна «Производительность» натиснути на кнопку «Добавить», яка має позначення «+» та у вікні, що з'явиться, у розділі «Объект» вибрати лічильник «Network Interface - мережевий інтерфейс» Ретельно перевірити частоту, з якою здійснюється отримання та відправлення пакетів через мережевий інтерфейс.(рис.4). 2.3. За допомогою лічильника Server/Work Item Shortage виконати перевірку обробки сервером мережевих запитів. Зазначений лічильник відслідковує дані щодо черги мережних запитів від користувачів. Якщо сервер перевантажений, то запит від користувачів може бути відкладений (рис.5.).

Примітка: В залежності від версії ОС сервера назва лічильника може бути інша.



Добавить счетчики	? ×
О Использовать локальные счетчики	Добавить
 Выбрать счетчики с компьютера: 	Закрыты
\\SM000M8040	
Объект:	Объяснение
Network Interface]
О Все счетчики	C Все вхождения
Выбрать счетчики из списка	 Выбрать вхождения из списка:
Packets Received Non-Unicast/sec Packets Received Unicast/sec Packets Received Unknown Packets Received/sec Packets Sent Non-Unicast/sec Packets Sent Unicast/sec Packets Sent/sec Packets Sent/sec	Intel(R) PRO Adapter Глобальный интерфейс (PPP_SLIP) Интерфейс внутреннего замыкания

Рис.4. Вибір лічильників для розрахунку трафіка локальної мережі

2.4. Здійснити аналіз мережевої активності компонентів серверу Redirector, за допомогою лічильника Network Errors (рис.6) та Current Commands, где: Network Errors – активність виникнення мережевих помилок, Current Commands – визначає кількість команд, які знаходяться у черзі до Redirector. Якщо число більше, ніж одна команда на один мережевий адаптер, то Redirector може бути вузьким містом у системі. Це виникає у зв'язку з появою суттєвих мережевих помилок. Поява таких помилок свідчить про необхідність проведення додаткових досліджень. Для з'ясування причин низької продуктивності необхідно використовувати журнал повідомлень ОС сервера Event Log.

Выбрать счетчики с компьютера:		
\\SM000M8040	•	
Объект:		
Server	•	
О Все счетчики		¢
Выбрать счетчики из списка		ē
Pool Paged Failures Pool Paged Peak Server Sessions Sessions Errored Out Sessions Forced Off Sessions Logged Off Sessions Timed Out Work Item Shortages		

Рис.5. Вибір лічильника сервера

💿 Выбрать счетчики с компьютера:	
\\SM000M8040	•
Объект:	
Redirector	-
О Все счетчики	
Выбрать счетчики из списка	
File Read Operations/sec File Write Operations/sec	
Network Errors/sec Packets Received/sec Packets Transmitted/sec	
Packets/sec Read Bytes Cache/sec Read Bytes Network/sec	•

Рис.6. Вибір лічильник Network Errors

2.5. Виконати перевірку завантаженості локальної мережі вузла, а саме, продуктивності обміну файлами між сервером та ПЕОМ користувача. Для цього

необхідно запустити програмне забезпечення **Performance Monitor** та додати лічильники **Reads Denied/sec и Writes Denied/sec** для *аналізу завантаженості локальної мережі вузла*. Якщо під час аналізу виявлено не нульові лічильників **Reads Denied/sec и Writes Denied/sec**, це свідчіть про те, що ПЕОМ, з якими здійснюється обмін, має проблеми оперативної пам'яті. (рис.6).

2.6. За допомогою лічильників **Pool Nonpaged Failures** та **Pool Paged Failures**. перевірити кількість *фізичної пам'яті сервера* (рис.8). Любі значення лічильників свідчать про те, у що сервера недостатньо фізичної пам'яті.

2.7. Після закінчення робіт здійснити заходи з віддалення лічильників. Для цього у вікні «Системный мониторинг» на правій половині вікна активізувати лівою кнопкою миші необхідний лічильник, далі натиснути на кнопку «Удалить», яка має позначення «Х», після чого необхідно ретельно перевірити стан відключення лічильників.

Добавить счетчики		
О Использовать локальные счетчики		
Выбрать счетчики с компьютера:		
\\SM000M8040	•	
лания стального пользования с пользовани		
Bedrester	-	
	<u> </u>	_
О Все счетчики		0
💿 Выбрать счетчики из списка		\odot
Read Bytes Paging/sec		Г
Read Uperations Random/sec		
Read Packets/sec		
Reads Denied/sec		
Reads Large/sec		
Server Disconnects	T	1
Joerver rieconnects		Ľ

Рис.7. Від вікна лічильника

О Использовать локальные счетчики	
Выбрать счетчики с компьютера:	
\\SM000M8040	•
Объект:	
Server	•
О Все счетчики	
 Выбрать счетчики из списка 	
Pool Nonpaged Failures Pool Nonpaged Peak Pool Paged Bytes Pool Paged Failures Pool Paged Peak Server Sessions Sessions Errored Out Sessions Forced Off	•

Рис.8. Від вікна лічильника Pool Nonpaged Failures

3. Моніторинг роботи Active Directory контролеру домену.

3.1. На панелі задач операційної системи сервера контролера домену натиснути на кнопку «Пуск», далі «Настройка», «Панель управления», «Администрирование», вибрати «Производительность». У вікні «Производительность», активізувати розділ «Системный монитор». Послідовно за допомогою лічильників, які наведені у таблиці, виконати технологічні операції з моніторингу роботи Active Directory контролера домену.

3.2. Після закінчення робіт здійснити заходи з віддалення лічильників. Для цього у вікні «Системный мониторинг» на правій половині вікна активізувати лівою кнопкою миші необхідний лічильник, далі натиснути на кнопку «Удалить», яка має позначення «Х», після чого необхідно ретельно перевірити стан відключення лічильників.

Завдання на виконання лабораторної роботи

1. Перевірити працездатність операційної системи Windows ПЕОМ користувача на віртуальної машині за допомогою програмного забезпечення **OracleVBox**, у разі необхідності здійснити налаштування її роботи.

2. Перевірити працездатність операційної системи Windows Server користувача на віртуальної машині за допомогою програмного забезпечення OracleVBox.

3. Перевірити працездатність операційної системи Windows Server користувача віртуальної машині у режимі контролеру домену.

4. Перевірити за допомогою утиліти командної строки «ping» із зазначенням ІР адреси серверу зв'язок між ПЕОМ користувача та контролером домену. (наприклад ping 192.168.10.6 - де 192.168.10.6 ІР адреса сервера).

5. Забезпечити безперервність зв'язку між ПЕОМ користувача та контролером домену. Для цього на ПЕОМ користувача запустити команду ping наприклад ping 192.168.10.6 - t, де 192.168.10.6 IP адреса сервера

6. Перевірити функціонування та величину завантаження локальної мережі між ПЕОМ користувача та контролером домену за допомогою програми «Диспечер задач»

7. Виконати перевірку величини завантаження контролеру домену на базі OC Window Server 2012/2016 за допомогою програмного забезпечення «**Performance Monitor**», використовуючи необхідні лічильники.

8. Здійснити моніторинг роботи програмного забезпечення Active Directory контролеру домену.

9. За результатами робіт підготуйте звіт щодо повноти виконання технологічних операцій з моніторингу мережі та контролеру домену.

ЗРАЗОК ЗВІТУ

	Назва лічильника		
N⁰	(мовою операційної	Пояснення (мовою операційної системи, що	Значення параметра, що отримане під час
з.п.	системи, що	встановлена на вузлі)	аналізу
	встановлена на вузлі)		
1	NTDS/DS Search sub- operations/sec	Использование ресурсов системы	
2	% Processor Time	Процент времени работы процессора службой Active Directory. Увеличение значения указывает на то, что новое приложение обращается к этому контроллеру домена, или что больше клиентов было добавлено к сети.	
3	NTDS/ LDAP Client Sessions	LDAP сеансы клиентов. Указывает текущее количество клиентов, связанных с контроллером домена. Его увеличение указывает на то, что другие машины не выполняют свою работу, перегружая этот контроллер домена.	
4	Процесс/ Private Bytes	Личные байты. Отслеживает объем памяти, используемой контроллерами домена.	

		Виртуальные байты. Используется для определения	
5	5 He average Virtual Dates	того, что Active Directory выполняется при нехватке	
5	Tipoleec/ virtual Byles	виртуального адресного пространства памяти, что	
		указывает на утечку памяти	
	NTDS/DDA Outhourd	Исходящие несжатые DRA байты. Указывает	
6	NIDS/DRA Outbound Bytes Not Compressed	количество реплицируемых данных, выходящих из	
	Dytes Not Compressed	этого контроллера домена.	
7	NTDS/NTLM	Указывает количество клиентов в секунду, которые	
Authentications	аутентифицируются на контроллере домена.		
0	Mamany	Высокая степень ошибок страницы указывает на	
0	Memory	недостаточную физическую пам'ять.	
	Discrete al Distr / Comment	Отслеживает объемы файлов Ntds.dit и .log.	
9	DiskQueue	Указывает, что имеется отставание дисковых запросов	
	DiskQueue	ввода/ вывода.	

Примітка: Назва лічильників може бути змінена в залежності від версії операційної системи Windows

Контрольні питання (відповісти письмово)

1. Методика визначення максимальної кількості активних сеансів на контролері домену.

2. Порядок перевірки функціонування локальної мережі та величини її завантаження.

3. Призначення, склад програми «Диспетчер задач». Методика перевірки завантаженості роботи мережі.

4. Призначення програмного забезпечення Active Directory. Місце розміщення програмних компонентів Active Directory на сервері. Порядок перевірки розміру бази облікових записів.

5. Описати склад та призначення компонентів Active Directory контролеру домену.

6. Порахувати основні лічильники та описати їх призначення щодо моніторингу роботи контролеру домену.

Лабораторна робота №6

Робота з доменними груповими політиками в MS Windows Server

Метою роботи є вивчення понять групової політики MS Windows Server, отримання практичних навиків щодо створення та налаштування доменних групових політик операційної системи Windows Server.

Технічне забезпечення занять

1. Персональне робоче місце студента (ПЕОМ на базі віртуальної машини) зі встановленим загальносистемним програмним забезпеченням (OC Windows)

2. Програмне забезпечення віртуалізації OracleVBox.

3. Програмне забезпечення контролеру домену ОС Window Server 2012/2016.

Питання, що відпрацьовуються на занятті

- 1. Налаштування групових політик контролеру домену.
- 2. Створення об'єктів домену та призначення обмежень.

Приклад виконання завдань:

1. В оснастці «Computers and Users» створити новий підрозділ «Organization Unit». Створити два підрозділи «Teachers», «Students». В «Teachers», «Students» створити по користувачу Teacher_G_N_1 та Student_G_N_1 відповідно, де G – номер групи, N – номер варіанта (рис.1).

🛃 Управление групповой политикой							_ [] ×
🛃 <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>О</u> кно <u>С</u> правка							- 8 ×
🗢 🔿 🙍 🖬 🗎 💥 🗊 🧕 🖥 🖬							
III Управление групповой политикой □ Д Лес: testdomain.com □ III Омены	Групп Связа	ы нные объекты групповой	й политики	Наслед <mark>ование груг</mark>	повой политики	Делегирование	1
🖃 🏥 testdomain.com	<u></u>	Порядок ссылок 🔺	Объект г	рупповой политики	Принудительный	Связь включена	Стат
 ☐ Default Domain Policy ☐ Domain Controllers ☐ Путпы ☐ Пользователи ④ Рабочие станции ☐ Рабочие станции ☐ Объекты групповой политики ☐ Default Domain Policy ☐ Default Domain Policy ☐ Default Domain Policy ☐ Default Pomain Policy ☐ Default Pomain Policy ☐ Политика аудита 10 литика аудита ☐ Фильтры WMI ☐ Сайты № Моделирование групповой политики 	41 4 F N	1	Полит	ика аудита	Het	Да	Вклн

Редактор локальной групповой политики

Файл Действие Вид Справка

	1144					
>	1	Windows Hello для бизне А	Состояние	Состояние	Комментарий	^
	-9	Windows Messenger	Общее диалоговое окно открытия файлов			
	-9	Windows PowerShell	🔛 Панель кадра проводника			
	19	Быстрый поиск	Предыдущие версии			
5	19	Виртуализация средств в	Отключить отображение эскизов и отображать только з	Не задана	Нет	
	19	Гаджеты рабочего стола	Отключить отображение эскизов и отображать только з	Не задана	Нет	
	1	Диспетчер вложений	🗄 Отключить кэширование эскизов в скрытых файлах thu	Не задана	Нет	
>	1	Диспетчер окон рабочег	🗄 Не показывать центр начальной настройки при входе по	Не задана	Нет	
	1	Добавить компоненты в	🗈 Включить классическую оболочку	Не задана	Нет	
	19	Звукозапись	🗄 Запрашивать подтверждение при удалении файлов	Не задана	Нет	
	1	Календарь Windows	🖹 Место, где располагаются все файлы определения библ	Не задана	Нет	
>	[°]	Консоль управления (МР	🗈 Отключить прямую привязку к IPropertySetStorage без пр	Не задана	Нет	
	r"	Магазин	🗈 Отключить возможности библиотеки Windows, использ	Не задана	Нет	
	r"	Найти	Отключить известные папки	Не задана	Нет	
	C	Общий сетевой доступ	🗄 Отключить отображение предыдущих поисковых запрос	Не задана	Нет	
	1	Отзыв файлов	🗄 Разрешить использование только пользовательских или	Не задана	Нет	
>		Отчеты об ошибках Winc	🗈 Запускать проводник со свернутой лентой	Не задана	Нет	
		Параметры входа Windo	🗄 Отключить отображение фрагментов в режиме просмот	Не задана	Нет	
		Параметры презентации	🗄 Не отслеживать ярлыки оболочки при перемещении	Не задана	Нет	
		Планировщик заданий	🗄 Максимальная длина списка «Недавние документы»	Не задана	Нет	
)		Планшет	Удалить возможности записи компакт-дисков	Не задана	Нет	
	-3	Политики автозапуска	Отключить кэширование эскизов изображений	Не задана	Нет	
	-9	Пользовательский интер	🗄 Запретить изменение видеоэффектов для меню	Не задана	Нет	
	19	Пользовательский интер	🗄 Запретить изменение указателя клавиатурного вызова	Не задана	Нет	
2	-9	Проводник Проигрыватель Windows	🗈 Удалить вкладку DFS	Не задана	Нет	
	-3	Рабочне папки	🗄 Скрыть выбранные диски из окна «Мой компьютер»	Не задана	Нет	
	19	Расположение и датчики	🗄 Скрыть значок «Вся сеть» в папке «Сеть»	Не задана	Нет	
	19	Редактор метода ввода	🗄 Удалить меню «Файл» из проводника	Не задана	Нет	
	19	Сборки для сбора данны	🗄 Запретить открывать окно «Параметры папок» с помощ	Не задана	Нет	
\$	-9	Службы удаленных рабо	Удалить вкладку «Оборудование»	Не задана	Нет	
1	19	Совместимость приложе	E Скрыть команду «Управление» из контекстного меню пр	Не задана	Нет	
	1	Содержимое облака	Удалить «Общие документы» из окна «Мой компьютер»	Не задана	Нет	
	-	Среда выполнения прил	Удалить команды «Подключить сетевой диск» и «Отклю	Не задана	Нет	
	19	Установщик Windows	Не перемещать удаляемые файлы в корзину	Не задана	Her	
	19	Пветовая система Windo 🗡				*
		>	<u>\Расширенный \Стандартный /</u>			

Рис.1. Вікно редактору групових політик контролеру домену

P O 🤅 🗎 🚺 占 🧾

 \pm

- 0 X

^ ∰ 48 ENG 27.04.2018 □



Рис.2. Створені об'єкти групової політики відповідних OU

2. У новостворених GPO виставити наступні обмеження для користувачів: «Students» (рис.3):

- заборонити доступ до панелі керування і управління параметрами комп'ютера;

- заборонити запускати «Диспетчер задач»;

-заборонити запис на портативні пристрої;

- видалити посилання на папку «Игры»;

- заборонити можливість підключення до віддаленого робочого столу;

-заборонити можливість видалення програм з меню «Пуск».

-заборонити використання інтерфейсу командного рядку.



Рис.3. Вид обмеження для користувачів підрозділу контролеру домену 3. Для «**Teachers**»: заборонити використання інтерфейсу командного рядку; заборонити можливість підключення до віддаленого робочого столу; заборонити доступ до панелі керування і управління параметрами комп'ютера.

4. Перевірити правильність налаштувань, виконавши вхід у домен з робочої станції використовуючи облікові записи створені у п.1 (рис.4 - рис.5)



Рис.4. Вхід в систему під записом користувача Student G N 1



Рис.5.Результат встановлених обмежень

Завдання на виконання лабораторної роботи

1. Перевірити працездатність операційної системи Windows ПЕОМ користувача на віртуальної машині за допомогою програмного забезпечення **OracleVBox**, у разі необхідності здійснити налаштування її роботи.

2. Перевірити працездатність операційної системи Windows Server користувача на віртуальної машині за допомогою програмного забезпечення OracleVBox.

3. Перевірити працездатність зв'язку між віртуальною машиною користувача та контролером домену. У разі несправності усунути помилки.

4. Переглянути компоненти контролеру домену за допомогою оснастки «Computers and Users», створити два підрозділу «Fakultet, Kafedra»

5. Встановити обмеження для новостворених GPO у відповідності до п.2 лабораторної роботи.

6. Перевірити правильність налаштувань, виконавши вхід у домен з робочої станції використовуючи облікові записи створені у п.4.

Контрольні питання (відповісти письмово)

1. Призначення групових політик контролері домену.

2. Призначення та порядок налаштування групових політик домену що призначаються по замовченням.

3. Методика створення об'єктів групової політики контролеру домену.

4. Описати склад та призначення адміністративних шаблонів групових політик контролеру домену.

5. Описати особливості порядку успадкування та пріоритетності використання доменних групових політик.

Лабораторна робота №7

настройка брандмауера OC Windows

Метою роботи є вивчення роботи та виконання операцій з налаштування деяких додаткових параметрів брандмауера OC Windows.

Технічне забезпечення занять

1. Персональне робоче місце №1 студента (ПЕОМ на базі віртуальної машини) зі встановленим загальносистемним програмним забезпеченням OC Windows 10.

2. Програмне забезпечення віртуалізації OracleVBox.

3. Програмне забезпечення ОС Window 10, встановлене на другої віртуальної машині (персональне робоче місце №2 студента).

Питання, що відпрацьовуються на занятті

1. Налаштування роботи брандмауера ОС Windows

2. Створення правил роботи з програмним забезпеченням за допомогою правил брандмауера ОС Windows.

Приклад виконання завдань:

1. На комп'ютері №1 натиснути правою кнопкою миші на робочому столі, далі вибрати New > Folder (Создать> Папку). (рис.1). Задайте ім'я нової папки - Сізсо.



Рис.1 Створення нової папки

2. Натиснить правою кнопкою миші на папці Cisco і виберіть «Share with > Advanced sharing > Advanced Sharing (Загальний доступ>

Розширена настройка загального доступу> Розширена настройка загального доступу). Відкриється вікно "Advanced Sharing" («Розширена настройка загального доступу») - (Рис.2).

	the second s
Nativoli Pie and Folder Sharing Orece Mit Shared Usevent Fahr Mit Shared Strand Set outure personal sector advanced Sharing Set outure personal sector advanced sharing splicing	Advanced Sharing
Paperusid Actention Resple without a user account a carr accessificides shared with To change the sating, use the	(Astronome) Castrop)

Рис.2 Розширена настройка загального доступу

3. Надайте спільний доступ до цієї папки, використовуючи ім'я за замовчуванням **Cisco**.

4. На комп'ютері №2 натисніть кнопку Start> (Пуск>), виберіть пункт Control Panel > Network and Sharing Center > Network (Панель керування> Центр керування мережами і загальним доступом> Мережа). Двічі натисніть комп'ютер №1 та перевірте наявність папок у відповідності до рис 3.



Рис.3 Вигляд папок загального доступу

5. Перейдіть до брандмауера на комп'ютері №1 ОС Windows.

6. Виберіть Start > Control Panel > System and Security > Windows
Firewall (Пуск> Панель керування> Система і безпека> Брандмауер
Windows) – рис. 4 Індикатор брандмауера показує стан брандмауера.
Стандартний режим "ON" («Включено»).



Рис. 4 Вікно брандмауера на комп'ютері №1 ОС Windows.

7. Перейдіть за посиланням Allow a program or feature through Windows Firewall (Дозволити запуск програми або компонента через брандмауер Windows). – рис.5



Рис. 5 Вікно брандмауера на комп'ютері №1 ОС Windows.

8. Відкриється вікно "Allowed Programs" ("Дозволені програми»).

рис 6.

		I. Warman) 3 1
OUT	 Windows Friendline Allowed Programs 	* + Scenti Ca	Hope Paris	P
File Edit	View Tools Help			
rie tol	Allow programs to communicate through Windows To add, change, or remove allowed programs and ports, click Chang What are the risks of allowing a program to communicate? Allowed programs and features: Name Demoti Gube - Centers Replays (Uses HTTM Demoti Gube - Hosted Cache Client (Uses HTTPS) Demoti Gube - Peer Discovery (Uses WSD) Concernation a Florench Discovery (Uses WSD)	Firewall a settings.	Public +	
	Connector Protection Projector Connector Projector Connector Protection Contributed Transaction Contributed Transaction Contributed File and Pinter Sharing HermaGroup COSI Service Key Management Service Herdia Canter Estandars		•	
		Ostails Allow and OK	Remove	

Рис.6. Вікно брандмауера на комп'ютері №1 ОС Windows.

9. Для програм і служб, що не блокуються брандмауером Windows, будуть встановлені прапорці. Можна додавати застосунки до цього списку. Це може бути необхідно, якщо у клієнта є застосунок, який вимагає з'єднання з зовнішньою мережею, але з якоїсь причини брандмауер Windows не може виконати настройку автоматично. Для завершення даної процедури необхідно увійти в систему на цьому комп'ютері з правами адміністратора.

10. Перейдіть за посиланням What are the risks of allowing a program to communicate? (Які ризики становить дозвіл зв'язку для програми?).

11. Відкриється вікно "Windows Help and Support" («Довідка та підтримка Windows»). – див. рис. 7.



Рис.7. Вікно довідки

12. Закрийте вікно "Windows Help and Support" («Довідка та підтримка Windows»).

13. З комп'ютера №1 виконайте наступні дії: натиснути вікно "Allowed Programs" ("Дозволені програми»), щоб активувати його. Рис.8.



Рис. 8 Вид вікна «Дозволені програми»

14. Для скасування винятку зніміть прапорець File and Printer Sharing (Загальний доступ до файлів і принтерів)> OK.

15. На комп'ютері №2 виконайте наступні дії: Відкрийте мережне підключення до комп'ютера №1.

16. Послідовно виберіть Start > Control Panel > Network and Sharing Center > Network (Пуск> Панель керування> Центр керування мережами і загальним доступом> Мережа). – рис.9.



Рис.9 Вікно мережі комп'ютеру №2

17. З комп'ютера №1 виконайте наступні дії: Для скасування винятку встановіть прапорець «File and Printer Sharing (Загальний доступ до файлів» і принтерів)> і натисніть ОК.

18. На комп'ютері №2 виконайте наступні дії: Оновіть вікно Network
 (Мережа) та здійснити з'єднання до комп'ютера №1.

19. Виберіть Start > Control Panel > System and Security > Administrative Tools > Windows Firewall (Пуск> Панель керування> Система і безпека> Адміністрування> Брандмауер Windows) в режимі Advanced Security > Inbound Rules (Підвищена безпека> Правила для вхідних підключень). Рис 10.

Windows Resevel with Advanced	Internet Roles	100 million					Action
Ministend Rules Outbound Rules Connection Security Rules Maintaining	Neme Core Networking - Time Exceeded IICMP/Grin Distributed Transaction Coordinator (PPC) Distributed Transaction Coordinator (PPC) Distributed Transaction Coordinator (PPC-IPM/AP) Distributed Transaction Coordinator (PC-IPM/AP) Distributed Transaction Coordinator (PC-IPM Distributed Transaction Coordinator (PC-IPM)	Scoup Core Networking Distributed Tensection Cool Distributed Tensection Cool Distributed Tensection Cool Distributed Tensection Cool Distributed Tensection Cool	Picifie All Densin Private - Centein Private - Densin Private -	Enclod Yes Ne Ne Ne Ne Ne Ne Ne	Artise Artes Artes Artes Artes Artes Artes Artes Artes	1 (10)	interest Re ↓ files ↓ files ↓ files ↓ files ↓ files ↓ files ↓ files
	File and Printer Sharing (Scho Request - ICMP-4-le) File and Printer Sharing (JLININ1-JDP-4r) File and Printer Sharing (JLININ1-JDP-4r) File and Printer Sharing (JLI-Distgram-3r) File and Printer Sharing File And	Disable Rule Cut Cony Delete Propulsion Help Propulsion Pla and Fernier Sharing	Demiin Public Private Demiin Public Demiil Private Demiin Public Private	Nac Nac Nac Nac Nac Nac Nac Nac Nac Nac	Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow		Supert. Help Help Help Help Cot La Copy Cot La Copy Nape.

Рис.10 Вікно «Правила для вхідних підключень»

20. Розгорніть вікно, щоб можна було побачити повне ім'я правил для вхідних підключень. Знайдіть Files and Printer Sharing (Echo Request – ICMPv4-In) («Загальний доступ до файлів і принтерів (ехо-запит - вхідний трафік ICMPv4)»). Натиснути правило правою кнопкою миші, виберіть Properties > Advanced> (Властивості> Додатково>) натисніть кнопку Customize (Налаштувати). – рис.11

General Protocols and Pots		Programs and Services		Computers
		Scope	Advanced	Upers
	ocity profile Domain Private Public	e is which the side a	and we	
artaca tor	eofy the init	leface types to whic	n this Custor	*re
Ches a serve	and the second second second second			
- 5	CORDING	is biterfece Types		
-	The rule	te Interfece Types apples to proveds terface types reinterfece types	ene on the following	a interfaces type
1212 (2) 40	The rule	e brieriece Types e apples to connects terface types ne néerlece types Local anse retrisorie Rende access Mastess	ana an 2n fallanny	a interfaces type

Рис.11. Вікно загального доступу до файлів і принтерів

21. На вкладці Advance («Додатково») відображається профіль, який використовується комп'ютером, а у вікні "Customize Interface Types" («Налаштування типів інтерфейсів») відображаються різні підключення, налаштовані на комп'ютері. Натисніть ОК.

22. Перейдіть на вкладку **Programs and Services** (Програми та служби). Відкриється вікно "Customize Service Settings" («Налаштування параметрів служби»). – рис. 12.

Victocols and Ports	Scope	Advanced	Users	
General Programs and Service		VICES	80 Computers	
rograme				
IN Allorogram	ns that meet the spe	offed conditions		
This proof	atti			
1		Brue		
L		In ware		
ervices				
Specify the se	rvices to which this	rule Settir	IDS	
applies.		ALC: Labore		
unite Casting Catting	-			
inite service setting	1900)			
ly this rule as follows :				
Apply to all programs a	nd services			
Analy to constant with				
which to services exit.				
Apply to this service:				
Name			Short Name	
🔍 ActiveX Installer (AxinstSV)		AxinstSV	
Adaptive Brightne	55		SenarSvc	
S Application Expen	ence		AaLookupSvc	
S. Application Identit	y		AppIDSvc	
S& Application Inform	ation		Appinto	
The American Statement	Galeway Service		ALG	
all upblication raye.	gement		App Mgmt	
Contraction Layer	A DURING THE CONTRACT OF A DURING THE DURING	te .	BITS	
 Application Layer Application Mana; Background Intell 	Igent Transfer Servi			
Application Layer Application Manaj Application Manaj Application Manaj Application Manaj Application Manaj Application Layer Application Layer	igent Transfer Servi Ine	2	BFE	
Application Layer Application Manay Background Intell	igent Transfer Servi ine 115 service short man	ne (example: evente	BFE	
Contraction Layer Contraction Manay Contraction Manay	igent Transfer Servi ine 11a service short man	ne (example: eventio	BFE 90)	
Contraction Layer Contraction Manay Contraction Manay	igent Transfer Servi Ine lite aervice short nan	ne (example: eventio	BFE	1

Рис.12. Вікно «Налаштування параметрів служби»

23. Перейдіть на вкладку **Protocols and Ports** (Протоколи і порти). Для настройки ICMP натисніть кнопку **Customize** (Налаштувати). Можна побачити меню, в якому налаштовуються винятки ICMP. –рис.13.

Customize JCMP Settings]
Apply this rule to the following Internet Control Message Protocol (ICMP) connections:	
C ALICMP types	
Specific ICMP types	
 Packet Too Big Destination Unreachable Source Quench Redirect Echo Request Router Advertisement Router Solicitation Time Exceeded Parameter Problem Timestamp Request Address Mask Request 	
This ICMP type:	
Type: 0 - Code: Any - Add	
Learn more about ICMP settings OK Cancel	

Рис.13. Вікно настройки ІСМР

24. У наведеному прикладі дозволяються вхідні ехо-запити, що дозволяє користувачам мережі перевіряти комп'ютер щодо визначення чи він в мережі. Це дає можливість відслідковувати, наскільки швидко передається інформація до комп'ютера і від нього.

Завдання на виконання лабораторної роботи

1. Перевірити працездатність операційної системи Windows ПЕОМ користувача на віртуальної машині №1 за допомогою програмного забезпечення **OracleVBox**, у разі необхідності здійснити налаштування її роботи.

2. Перевірити працездатність операційної системи Windows користувача на віртуальної машині №2 за допомогою програмного забезпечення OracleVBox.

Перевірити працездатність зв'язку між віртуальними машинами.
 У разі несправності усунути помилки.
4. Виконати пункти лабораторної роботи та здійснити перевірку роботи брандмауера операційної системи Windows.

Контрольні питання (відповісти письмово)

1. Призначення брандмауера операційної системи Windows.

2. Методика налаштування параметрів брандмауера операційної системи Windows на роботу щодо забезпечення доступу до ресурсів комп'ютера.

3. Опишіть основні вхідні та вихідні правила роботи брандмауера операційної системи Windows.

4. Призначення основного та швидкого режиму роботи брандмауера операційної системи Windows.

5. Призначення папки «Наблюдение» брандмауера операційної системи Windows.

6. Методика створення правил роботи брандмауера для програми.

7. Методика створення правил роботи брандмауера для порту.

Лабораторна робота №8

Встановлення та налаштування VPN з'єднання MS Windows Server

Метою роботи є освоєння навиків зі створення та налаштування VPNсервера на базі Windows Server.

Технічне забезпечення занять

1. Персональне робоче місце студента (ПЕОМ на базі віртуальної машини) зі встановленим загальносистемним програмним забезпеченням ОС Windows.

2. Програмне забезпечення віртуалізації OracleVBox.

3. Програмне забезпечення ОС Windows Server, встановлене на другої віртуальної машині.

Питання, що відпрацьовуються на занятті

1. Створення VPN сервера на базі ОС Windows 2012/2016 Server.

2. Виконати налаштування роботи VPN сервера із конфігуруванням портів та підтримки технології NAT.

Приклад виконання завдань:

Створення VPN сервера

1. Відкрийте службу "Маршрутизація і віддалений доступ" та активізуйте властивості сервера. (рис.1.)

👰 Маршрутизация	и удаленный доступ		_ O ×
Дойствно вна	(+ + 🗈 🖬 🕻	X 🗗 🗈 🖫 😭	
Структура	30 W SASH	ТЕSTЗ (покально)	
Маршрутизация и Состояние сер	удаленный доступ вера на)	Иня Интерфейсы нарырутизации В IP-нершрутизация	
— Э. Интерфен — Э. Р-карыр	Настранть п'яключить Отключить наршрути	перарутизецин и удатенный досту: зацию и удаленный доступ	
Все задачи	Все задачи		
	Вна		•
	Удалить Обновить Экопортировать списо	.	
	Свойктва		
	Справка		
			- 10

Рис.1. Властивості сервера

2. Встановити параметр "локальной сети и вызов по требованию", а також "сервер удаленного доступа (рис 2).



Рис.2. Параметри сервера

3. Зайдіть на вкладку "ІР", виберіть назву внутрішнього адаптера і створіть статичний пул адрес, відмінний від внутрішнього, який буде присвоюватися VPN-клієнтам. (рис. 3).

Свойства: П	5ТЗ (ло	кально)					? ×
Вощие Ба	зопасно	сть IP	AppleTak.	PPP .	Журнал	событий	
I Pasper I Bgane Haseave Cepsep C ripor I cran	шять IP+и нный IP-др может на гокол DH инаский	арщрутизан роступ с пря пресов соначать IP СP	цио адоставления адреса, исп в	ан канала ользуя:	но треби	ованию	
c		по	Числов	IP-appec	Маск	a	
<u>Да</u> Использу DNS-и WI	обезить Иге следу NS-серек	. Измен ющий адел	ить У пердля для мантов удал	дагить получения енного доо	адресов ступа.	s DHCP-,	
Адаттер:	none:	зователи				•	1
		[OK	Отм	0H0	Приме	нить

Рис.3. Властивості протоколу ІР

Новый диапазон адрес	08 <u>? ×</u>
Введите начальный IP-ад адресов в непрерывном	рес и либо конечный IP-адрес, либо число диапазоне.
Начальный IP-адрес:	192.168.1.1
Конечный IP-адрес	192.168.1.254
Количество адресов:	254
	ОК Отмена

Рис.4. Призначення пули адрес IP

4. Далі у вкладці "РРР" зніміть галочку з "Многоканальные подключения" – це прискорить роботу Інтернету.

Свойства: ТЕБТЗ (локально)	? ×
Общие] Безопасность] IP РРР [Журнал событий]	
Этет сервер жожет использовать указанные параметры протокола FPP. Политики удаленного доступа определяют параметры. используемые для каждого падключения.	
Многоканальные подключения	
Динаниическое управление пропускной способнастию (ВАРУВАСР)	
Расширения LCP	
Программное сжатие данных	
ОК Отмена Примен	ить

Рис.4 Вид закладки «РРР»

всех событий"

5. У вкладці "Журнал событий" виставіть параметр "вести журнал



Рис.5 Вид закладки «Журнал собітий»

Конфігурація портів

6. Зайдіть у властивості «Порты». За замовчуванням RRAS створить п'ять "PPTP", п'ять "L2TP" і один **"Прямой параллельный"**.

7. Для стабільної роботи сервера рекомендується видалити непотрібні порти (прямий паралельний, L2TP, i.т.д.) і створити необхідну кількість портів Їх має бути більше, ніж одночасних підключень.



Рис.6. Створення портів за допомогою вікна «Маршрутизация и удаленный

доступ»

Coc	йства: Порты			<u>? x</u>
Ę	Істройства			
	Маршругизация и удаленн устройства.	ый доступ используют п	еречислен	ные
	Устройство	Используется	Тип	Чись
	Минипорт WAN (PPTP)	RAS/Маршрутноацня	PPTP	5
	Минипорт WAN (L2TP)	RAS/Маршрутизация	L2TP	5
	Прямой параллельный	Маршругизация	Пар	1
				- 1
				- 1
				- 1
				- 1

Рис.7 Властивості портів системи

8. Видаляємо порти WAN(L2TP). Необхідно встановити необхідну кількість РРТР портів (кількість портів має бути більша, ніж планованих одночасних підключень).

Настройка устройства - Минипорт WAN (PPTP) 🤶 🔀
Можно использовать это устройство для запросов уделенного доступа или подключений по требованию.
🔽 Подключения удаленного доступа (только входящие)
Подключения по требованию (вкодящие и нокодящие)
Номер телефона этого устройства:
Можно задать предел числа портов для устройств, обеспечивающих поддержку нескольких портов.
Максимальное число портов: 128 🔹
ОК. Отмена

Рис. 8 Налаштування пристрою – «Минипорт (WAN)»

9. В результаті у вас з'явиться вікно –рис 9:

Евойства: Порты			<u>?</u> ×
Устройства			
Маршругизация и удаленн устройства.	ый доступ используют пе	речислен	ные
Устройство	Используется	Тип	Чно
Минипарт WAN (PPTP)	RAS/Маршрутизация	PPTP	128
Минипорт WAN (L2TP)	Her	L2TP	0
Прямой параллельный	Нет	Пар.,	1

Рис.9 Вікно властивостей «Порти»

Конфігурація NAT

10. Зайдіть у "ІР-маршрутизация"/"NAT-преобразование сетевых

адресов". Якщо ви збираєтесь надавати доступ тільки по VPN з'єднанню, тоді видаліть внутрішній інтерфейс, якщо ні – тоді залиште.

11. Якщо ви використовуєте Windows Server вам необхідно відключити **basic firewall**. Її використання при наявності Traffic Inspector може призвести до конфліктів. Для цього зайдіть у властивості зовнішнього підключення і відключіть.



12. Далі потрібно додати **RAS інтерфейс**. Для цього в командному рядку наберіть "netsh routing ip nat add interface Внутрішній (у англійській версії Windows "internal") private".

C:\WINNT\system32\cmd.exe	. 0 ×
C:\>netsh muting ip nat add interface Buyrpennum private	*
C: \}	_
	v.

13. Крім того необхідно заборонити прив'язку NetBios до інтерфейсу Внутрішній (internal), якщо він активний.

14. Якщо NetBios дозволений на цьому інтерфейсі, то сервер реєструватиме свої NetBios-імена з IP-адресами усіх інтерфейсів, на які є прив'язка цієї служби. Поява IP-адреси інтерфейсу Внутрішній (internal) в цих реєстраціях може призвести до проблем.

15. Для цього редактором реєстру в розділі HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesRemoteAccessP arametersIp додаємо параметр DisableNetbiosOverTcpip типу DWORD зі значенням 1. Службу потрібно перезапустити. Автоматично з'явиться RAS інтерфейс – рис 10.

🖗 Маршрутизация и удаленный доступ				_ 🗆 ×		
дейстене Вна 🛛 🕶 🖻 🖬 😭	1 🗟 🖳 😫					
Структура	НАТ - преобразование сетевых адресов					
В Маршрутизация и удаленный доступ	интерфейс т	Bcero conoct	Прибыванх	Biconsup		
Состояние сервера ТЕСТЗ (локально) Интерфойсы наршсу тюации Клижиты удаленного доступа (б) Порты Ринаршрутюация Статические наршруты Агент DHCP-ретрансляции БСМР МАТ - преобразование сетерык а Политика удаленного доступа	не провайсер	0	0	0		

Рис.10 Властивості вікна «Маршрутизация и удаленный доступ»

Створення клієнтів

16. Зайдіть у "Управление компьютером", далі в "Локальные пользователи и группы", "Пользователи". Створіть користувача, імена користувачів повинні співпадати з іменами клієнтів. Далі зайдіть на вкладку "Входящие звонки".

Свойства: User1	? ×
Общие Членство в группах Профиль Вкодящие звонки	
Разрешение на удаленный доступ (//PN или модем)	
🧭 Разрешить доступ	
С Запретить доступ	
С. В правление на основе политики удаленного доступа	
Просерять идентификатор:	
Ответный вызов сарвера	
Ответный вызов не выполняется	
 Устанавливается вызывающим (только для RAS) 	
Всегда по этому номеру;	
Бтатический IP-адрес тольсорателя	
Использовать статическую маршругизацию	
Определите маршруты, работеющие	
с вюдящим подключением.	
Закрыты Отмена Примен	ять

Рис. 11. Вікно властивостей користувача

Налаштування VPN з'єднання

17. В групі "Политика удаленного доступа" зайдіть у властивості «Разрешить доступ, если разрешены входящие подключения» - рис 12



Рис.12. Политика удаленного доступа

18. Натисніть кнопку "Изменить профиль..."

Свойства: Разрешить доступ, если разрешены вкодящие по 🎦 🗙
Параматры
Имя политики ить доступ, если разрешены виодящие подключения
Укажита условия, которое должно быть выполнено:
DajeAnd-Time-Flestrictions contercineyer "Bic U0100-24;00; TH D000-24;
Добавить Удалить Иоменить
Если пользователь соответствует условиям
Предоставить право удаленного доступа
Отказать в праве удаленного доступа
Доступ будат предоставлен в соответствии с указанным профилем, если только доступ не будет переопределен для конкретных пользователей.
Изменить профиль
ОК. Отмена Пряменить

Рис.13. Политика удаленного доступа

19. Зайдіть на вкладку "Проверка подлинности"

Изменение профиля коинутируемых подключений 💦 🔀
IP Многоканальное подключение
Проверка подлинности Шифрование Дополнительно
Ограничания по вкодящни звонкам
Разъединение при простое более: 1 мин.
Максимальная продолжительность сеанса 1 мин.
Ресрещить входящие подключения только в эти дни и время
Измените
Разрешить вход только по номеру:
Разрешить входящие звонки следующих типов
FDDI 🔺
Token Bing
Ц Беспроводная связь - IEEE 802.11
☐ Беспроводная связь - другая
ОК. Отмена Применить

20. Залишити два параметри перевірки справжності MS-CHAP для OC Windows і CHAP для інших OC.- рис.14

Изменение профиля коиму	зменение профиля коимутируемых подключений 🛛 🝸 💌		
IP [IP Многозанальное подалючение		
Ограничения по входящим звонкам			
Праверка подлинности	Шифрование	Дополнительно	
Выберите методы проверки подлинности, использувные для этого подключения. Протокол расширенной проверки подлинности (EAP)			
Выбериге приемиемый тип протокола для этой политики.			
Зашишенный ЕАР (РЕАР) 💌 Настроиты			
 Шифрованная проверка (Microsoft, версия 2, MS-CHAP v2) Шифрованная проверка подлинности Microsoft (MS-CHAP) Шифрованная проверка подлинности (CHAP) 			
Проверка открытым тестом (РАР, 5РАР)			
Доступ без проверки Разрешить удаленным клиентам РРР □ подключаться без согласования метода проверки подлинности.			
	DK. Dm	мана Применить	

Рис.14. Вікно зміни профілю

21. Далі зайдіть на вкладку "Шифрование", выберіть параметри шифрування. Усі виконані налаштування повинні бути ідентичними при налаштуванні VPN з'єднання у клієнтів, далі перезавантажити сервер.

1зменение профиля коммутируемых подключений 💦 🔀			
IP	Многоканальное подключение		
Опроничения по входящим авонком			
Проверка подлинности	и Шифровани	18 Даполнительно	
Примечание: эти парам службы маршрутизация Выберите уровня шифр IV Без шифрования IV Основное IV Стояков IV Самов стояков	атры шифрования п и и удаленного досту ования, разрешению	трименимы только для gna Windows 2000. не для этого профиля.	

Рис.15. Вікно зміни профілю

Завдання на виконання лабораторної роботи

1. Перевірити працездатність операційної системи Windows ПЕОМ користувача на віртуальної машині №1 за допомогою програмного забезпечення **OracleVBox**, у разі необхідності здійснити налаштування її роботи.

2. Перевірити працездатність операційної системи Windows користувача на віртуальної машині №2 на базі Windows Server 2012/2016.

Перевірити працездатність зв'язку між віртуальними машинами.
 У разі несправності усунути помилки.

4. Виконати пункти лабораторної роботи та здійснити перевірку працездатності VPN з'єднання між віртуальними машинами.

Контрольні питання (відповісти письмово)

1. Призначення та характеристика технології VPN.

- 2. Рівні реалізації VPN з'єднання.
- 3. Склад VPN.

4. Класифікація VPN.

- 5. Протоколи мережі, що використовує технологія VPN.
- 6. Недоліки технології VPN.
- 7. Приклади застосування технології VPN.
- 8. Характеристика технології ОрепVPN.
- 9. Види автентифікації, що засовуються у технології OpenVPN.
- 10. Типи операційних систем, де використовується OpenVPN.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАНЯТТЬ

1. Електронні та друковані інформаційні ресурси.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Exam Ref 70-742 Identity with Windows Server 2016. Published with the authorization of Microsoft Corporation by: Pearson Education, Inc.Copyright © 2017 by Pearson

2. Exam Ref 70-742 Identity with Windows Server 2016 Published with the authorization of Microsoft Corporation by: Pearson Education, Inc.Copyright © 2017 by Pearson Education Inc.

3. Mastering Windows Server 2016 Copyright © 2016 Packt Publishing

4. Т. Адельштайн, Б. Любанович. Системное администрирование Linux. //СПб:Питер, 2014. -288 с.

5. Колісніченко Д.Н. Linux – сервер своїми руками. СПб: //Наука и Техника, 2014 – 678 с.

6. Основи адміністрування LAN у середовищі MS Windows. Навчальний посібник / Б. А. Демида, К. М. Обельовська, В. С. Яковина. Львів: Видавництво Львівської політехніки, 2013.- 488 с

7. Р.Моринто, М.Ноэл и др. MS Windows Server 2012 Полное руководство. - М. изд. Вильямс -2013.-1456 С.

Кен Хендерсон. Профессиональное руководство по SQL Server.
 //Структура и реализация, 2012 – 1064 с.

9. Бруй В.В., Карлов С.В. Linux-сервер: пошаговіе инструкции инсталяции и настройки.//Москва.: Изд-во СИП РИАб 2012. – 572 с.

10. И.Ф. Астахова. SQL в примерах и задачах.// Учебное пособие, 2012 – 176 с.

 Рэнд Моримото, Майкл Ноэл, Омар Драуби, Росс Мистри, Крис Амарис - Microsoft Windows Server 2008 R2. Полное руководство, 2011 – 1455 с.

12. Душан Петкович. MS SQL Server. Руковоство для начинающих, 2009 – 743 с.